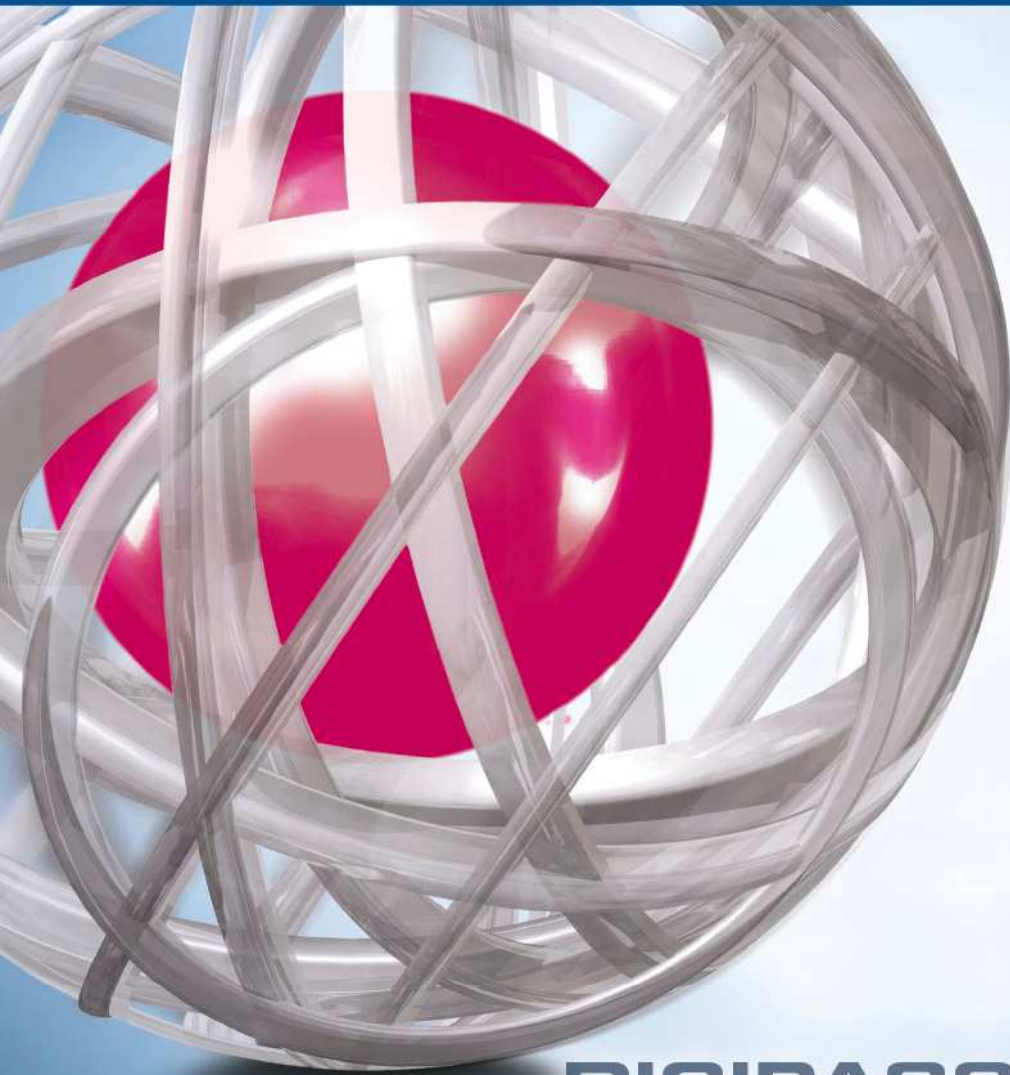




DIGIPASS Authentication for Microsoft Exchange ActiveSync 2007



DIGIPASS BY VASCO



The world's leading software company specializing in **Internet Security**

Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

Copyright

Copyright © 2010 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXsGUARD™™, DIGIPASS® and ® 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 Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.

Table of Contents

Disclaimer	1
Table of Contents	2
Reference guide	4
1 Overview.....	5
2 Technical Concepts	6
2.1 Microsoft	6
2.1.1 Windows 2008 Server.....	6
2.1.2 IIS 7	6
2.1.3 Exchange 2007.....	6
2.1.4 Windows Mobile	6
2.1.5 Exchange ActiveSync.....	6
2.2 VASCO.....	6
2.2.1 IDENTIKEY server or aXsGUARD Identifier.....	6
2.2.2 IDENTIKEY IIS basic Web filter	6
3 Exchange ActiveSync Configuration	7
3.1 Architecture.....	7
3.2 Windows 2008 server	7
3.3 Exchange 2007 configuration	7
3.4 IIS 7 configuration	8
3.5 Windows Mobile configuration	9
4 Solution	11
4.1 Architecture.....	11
4.2 IIS 7 configuration	11
4.3 Web filter configuration.....	13
4.4 IDENTIKEY server configuration	14
4.5 Test the solution	16

5 FAQ..... 18

5.1 Do I have to fill in an OTP at each time I want to synchronize? 18

5.2 Does the password in clear text cause any security issues..... 18

Appendix 19

Reference guide

ID	Title	Author	Publisher	Date	ISBN

1 Overview

This whitepaper describes how to enable strong authentication for users that use Microsoft Exchange ActiveSync(EAS) to access their E-mails on the Exchange server using their Windows Mobile handheld device.

2 Technical Concepts

2.1 Microsoft

2.1.1 Windows 2008 Server

Windows 2008 Server is used as Domain Controller (DC), Web server and Exchange server. All of those roles can also be fulfilled by several computers, it all depends on your own configuration.

2.1.2 IIS 7

The IIS 7 is the standard web server that is provided with Windows 2008 Server and will be used to publish the websites.

2.1.3 Exchange 2007

Exchange 2007 is the standard mail server of Microsoft. The mail server will provide us with the tools to make it possible to use Exchange ActiveSync.

2.1.4 Windows Mobile

Windows Mobile is the software that is used on Microsoft based handhelds. On the Windows Mobile we will use the pre installed, default mail client.

2.1.5 Exchange ActiveSync

ActiveSync (AS) is traditionally known as a synchronization tool used to synchronize a Windows Mobile device with your desktop/laptop. In order to use this you have to connect your handheld device to your desktop/laptop.

Outlook uses Exchange ActiveSync (EAS) in order to synchronize your mobile mail client on a handheld device using Windows Mobile, with the Microsoft Exchange server. Unlike AS on desktop, you only need a network connection. EAS will use the HTTP(s) protocol to connect the web server.

2.2 VASCO

2.2.1 IDENTIKEY server or aXsGUARD Identifier

IDENTIKEY Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

IDENTIKEY Server is supported on 32bit systems as well as on 64bit systems.

aXsGUARD Identifier is a standalone authentication appliance that secures remote access to corporate networks and web-based applications.



The use and configuration of an IDENTIKEY Server and an aXsGUARD Identifier is similar.

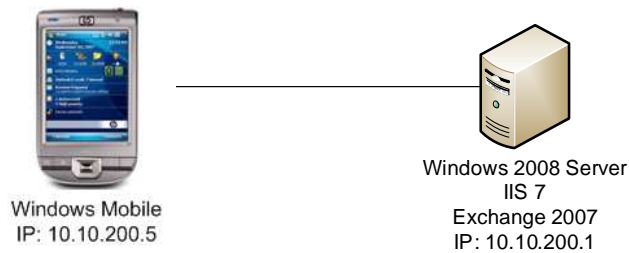
2.2.2 IDENTIKEY IIS basic Web filter

The IDENTIKEY IIS basic web filter is used to authenticate via the HTTP protocol.

3 Exchange ActiveSync Configuration

Before adding 2 factor authentication it is important to validate a standard configuration without One Time Password (OTP).

3.1 Architecture



The use of HTTPS (SSL) outside the scope of this integration guide.

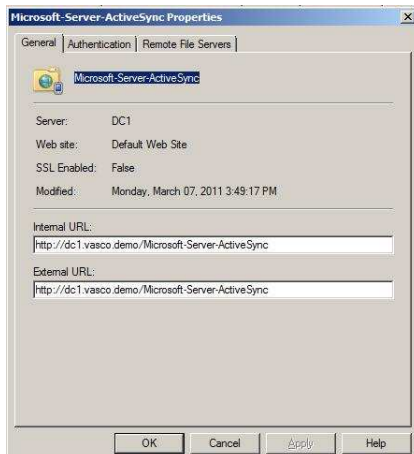
3.2 Windows 2008 server

The following base configuration is used

Roles	Domain Controller
	Web Server (Full install)
Extra installation	Exchanger 2007 (standard)

3.3 Exchange 2007 configuration

- Open **Exchange Management Console**
- Go to
 - **Server Configuration**
 - **Client Access**
 - **Exchange ActiveSync**
- Open **Microsoft-Server-ActiveSync**
- Fill in the **General settings**

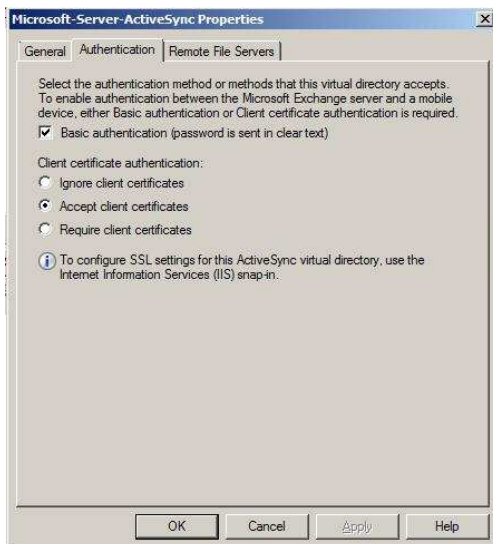


Internal URL: the url that will be used for internal usage

External URL: the url that will be used for external usage

In our case the same link is used for both

- Fill in the **Authentication settings**

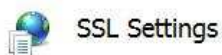


We will use Basic authentication. Basic authentication is a standard windows authentication with username and password sent in clear text.

3.4 IIS 7 configuration

Our setup is based upon HTTP, hence the use of certificates will be disabled. Please skip this step if you want to use certificates.

- Open **Internet Information Service (IIS) Manager**
- Go to
 - **DC1**
 - **Sites**
 - **Default Web Site**
 - **Microsoft-Server-ActiveSync**
- Open **SSL-Settings**



This page lets you modify the SSL settings for the content of a Web site or application.

- Require SSL
 - Require 128-bit SSL

- Client certificates:
- Ignore
 - Accept
 - Require

- Restart your **web server**

3.5 Windows Mobile configuration

For this example an emulator is used that is running Windows Mobile 6 and it is connected to the local network.



- **Start**
- **Messaging**
- **New E-mail Account**
- **Enter E-mail address**
- **Uncheck** "Try to get e-mail setting automatically from the internet"
- **Next**
- Your e-mail provider: **Exchange server**
- **Next**
- **Next**
- Server address: **dc1.vasco.demo**
- **Uncheck** "This server requires an encrypted (SSL) connection" (If you want to use ssl leave this enabled)
- If you get a warning click **ok**
- Fill in:



The user credentials are the standard windows logon credentials.

- **Next**
- **Finish**
- **Close**
- **Now you can send and receive mails**

The first time you are connecting to the exchange server, the device will ask



- Click **OK**

If you see this message



Everything is fine. Close the application and you can send/receive e-mails.

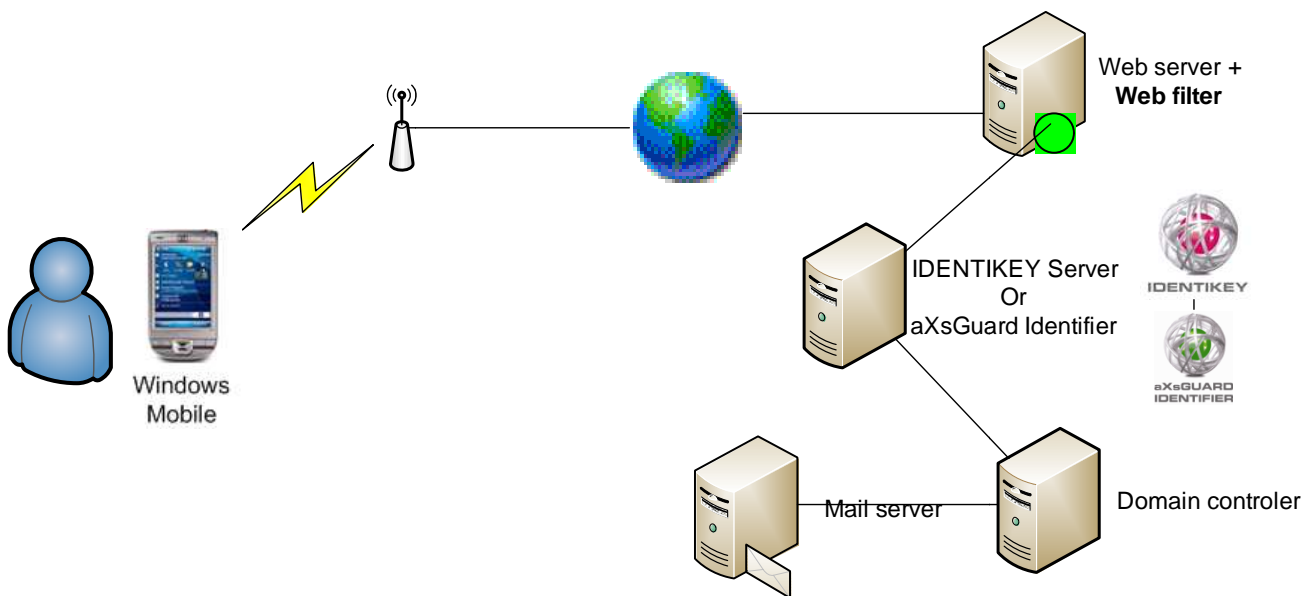
4 Solution

Install the IDENTIKEY Server and the IIS basic web filter on the server.



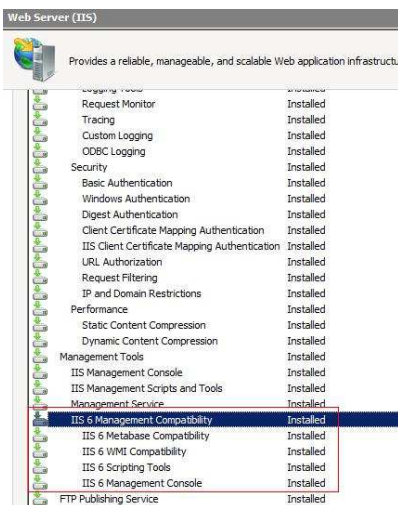
VASCO provides an installation guide together with IDENTIKEY server and the Web filter. In both cases a standard installation needs to be performed.

4.1 Architecture



4.2 IIS 7 configuration

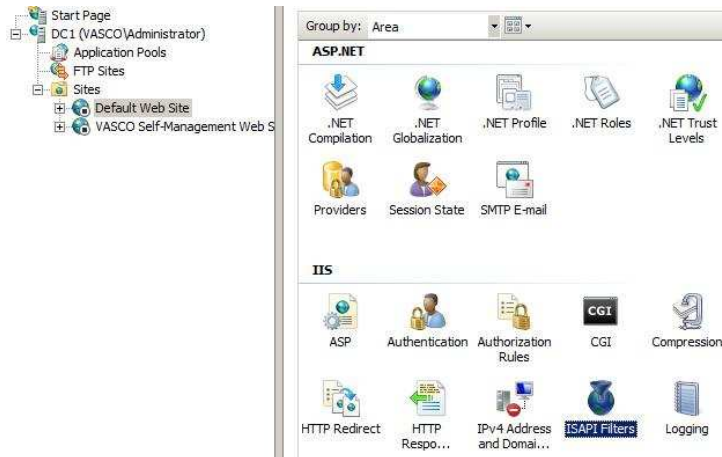
IDENTIKEY Server uses the IIS 6 Management Compatibility. You can activate this feature on the web server:



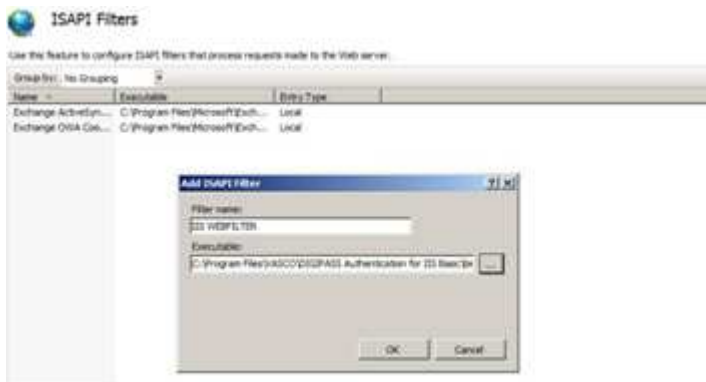
The **Internet Server Application Programming Interface (ISAPI)** is an N-tier API of Internet Information Services (IIS), Microsoft's collection of Windows-based web server services. The most prominent application of IIS and ISAPI is Microsoft's web server.

The ISAPI filter for the IIS web filter has to be added manually.

- Open **Internet Information Service (IIS) Manager**



- Open **ISAPI Filter**
- **Add** the filter



The default location of the VASCO ISAPI web filter is:

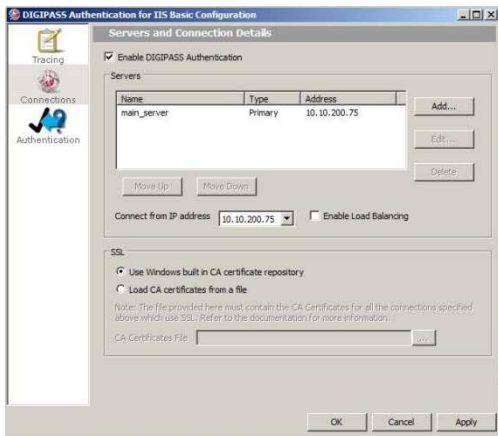
C:\Program Files\VASCO\DIGIPASS Authentication for IIS Basic\bin**dpiisfil.dll**

- **Restart** the web server

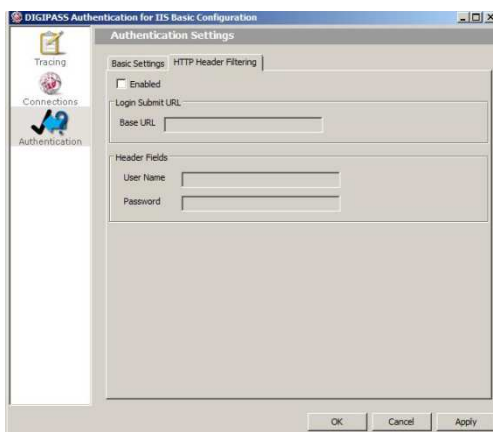
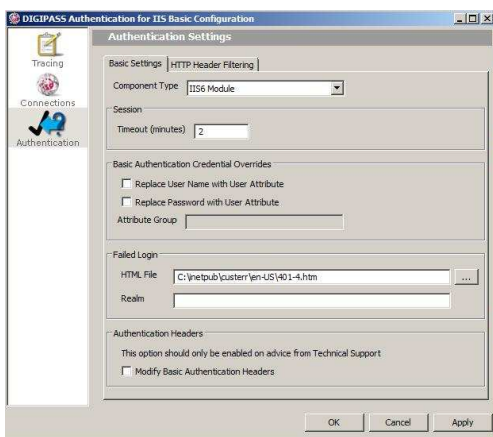
4.3 Web filter configuration

Start > All programs > VASCO > DIGIPASS Authentication for IIS Basic > DIGIPASS Authentication for IIS Basic Configuration

The only configuration that has to be done is to **Enable the Web Filter**.



Check: Enable DIGIPASS Authentication

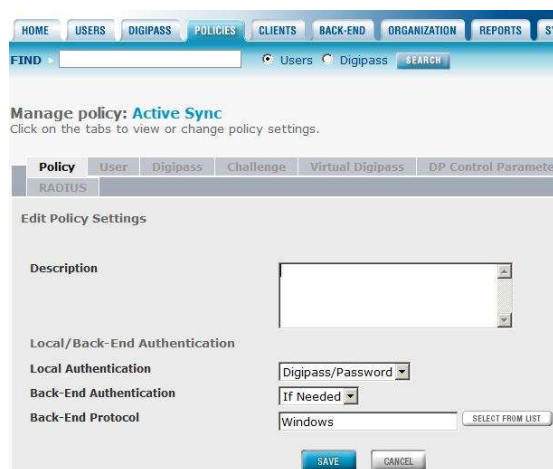


4.4 IDENTIKEY server configuration

- Open the **IDENTIKEY web admin**
- Add a new **policy**:



- Enter a **Policy ID**: Active Sync
- Inherits **From**: Base Policy
- **Open** the new policy and edit **POLICY**



Local Authentication: Digipass/Password – The IDENTIKEY Server will always carry out Local Authentication under this policy using Digipass Authentication or the static password. Back-End authentication may also be used with this setting.

Back-End Authentication: If needed – The IDENTIKEY Server will use Back-End Authentication under the following circumstances:

- Dynamic User Registration
- Self-Assignment
- Password Autolearn
- Requesting a Challenge
- Virtual Digipass OTP
- when request method involves a Static password authentication
- when verifying a Virtual Digipass password-OTP combination
- during the Grace Period
- Provisioning Registration

Back-End Protocol : Windows – Authentication against the Windows domain. This option is only available when IDENTIKEY Server is installed in the domain.

- **Save**
- Open tab **Users** and edit



Dynamic User Registration: Specifies whether the Dynamic User Registration (DUR) feature is enabled for the policy.

If this feature is used, when the IDENTIKEY Server receives an authentication request for a User for the first time and Back-End Authentication is successful, against the Windows Domain, it will create a Digipass User account automatically. If DUR is used in conjunction with Auto-Assignment, a Digipass will be assigned to the new User account immediately. This setting also determines whether the Provisioning Registration process is allowed to perform DUR or not.

Password Autolearn: Specifies whether the Password Autolearn feature is enabled for the policy.

This feature enables the IDENTIKEY Server to update the password stored in the Digipass User account when Back-End Authentication is successful.

This setting also determines whether the Provisioning Registration process will update the password or not after successful Back-End Authentication.

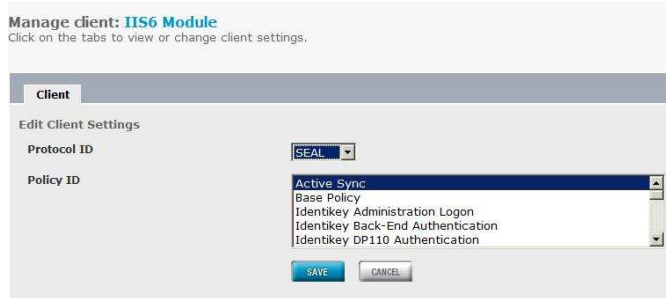
Stored Password Proxy: Specifies whether the Stored Password Proxy feature is enabled for the Policy. This feature can be used in conjunction with the Back-End Authentication Always setting and the Password Autolearn feature. With this combination, even though a Back-End Authentication check is done at every login, it is done using the password stored in the Digipass User account. Therefore the User does not have to enter it during their login, unless it has changed in the Back-End System. This mode of operation is referred to as Password Replacement.

- **Save**
- Go to **clients**

Administration Program	10.10.200.1	SOAP
IIS6 Module	10.10.200.1	SEAL
Identikey Windows Logon Client	default	SEAL
RADIUS Client	10.10.200.1	RADIUS

Normally you have to see a client "**IIS6 Module**" with a SEAL protocol.

- Connect the **Active Sync Policy** to the client



4.5 Test the solution

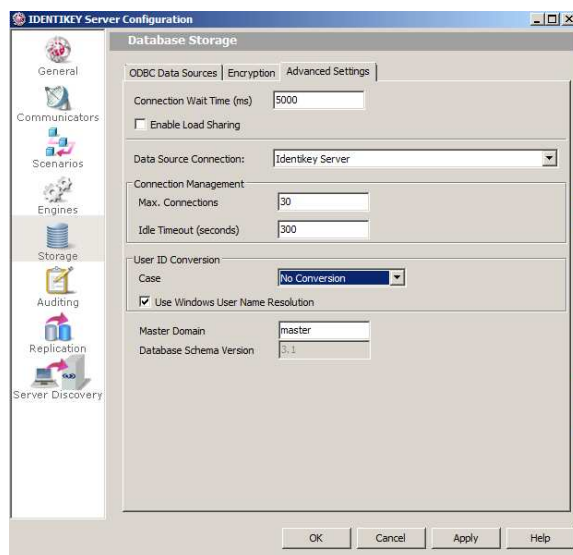
The handheld device will now authenticate using IDENTIKEY. This will change nothing to the standard authentication, the user (user1) will see no difference.

On the IDENTIKEY side a user account will be created.



The best practice is to classify the users in domains, these domains are the same as the domains used in the Domain Controller.

In Start > All programs >VASCO > Identikey Server >Identikey Server Condiguration



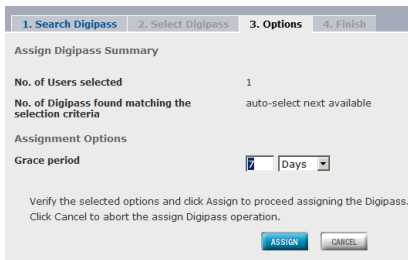
Enable the option: Windows name resolution

As long as there is no DIGIPASS assigned to the user, he will use his standard Windows logon password.

- Assign a DIGIPASS to the user



- Eventually enter search criteria
- Enter the grace period



Grace period is the period that a user can log in with his static password. The first time the user uses his DIGIPASS the grace period will expire.



Specify the number of days or weeks grace period the User has with the DIGIPASS



If the user needs to use the DIGIPASS immediately set the Grace period to **0 Days**

The next time Windows mobile will synchronize with the EAS, the device will prompt to enter a password.



- Fill in the **OTP**

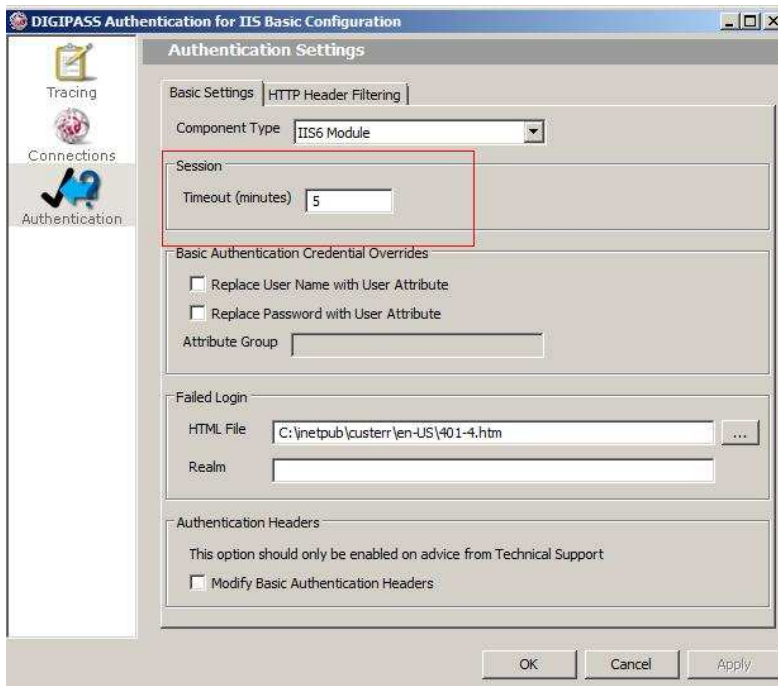


Save password has to be **enabled**, otherwise the device will constantly prompt to reenter a password

5 FAQ

5.1 Do I have to fill in an OTP at each time I want to synchronize?

Answer: No, the authentication will start a session, during this session the mobile device won't ask for a new password. A session is interrupted if the timeout passed or when the application is closed on the handheld devices.



5.2 Does the password in clear text cause any security issues

Answer: No, the **One Time Password** is generated using a unique key (defined in every DIGIPASS) and is unique for that particular Digipass and use. Stealing the **One Time Password** is useless because the password can only be used once (Like the name states).

Appendix

Downloads

Windows Mobile emulator:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=38c46aa8-1dd7-426f-a913-4f370a65a582&displaylang=en>