



THE AUTHENTICATION COMPANY

DIGIPASS Authentication for Microsoft ISA 2006

VPN Connections

With IDENTIKEY Server / Axsguard IDENTIFIER

Disclaimer

Disclaimer of Warranties and Limitations of Liabilities

This Report is provided on an 'as is' basis, without any other warranties, or conditions.

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.

Trademarks

DIGIPASS , IDENTIKEY, IDENTIFIER & AXSGUARD are registered trademarks of VASCO Data Security. All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Copyright

© 2010 VASCO Data Security. All rights reserved.

Table of Contents

DIGIPASS Authentication for Microsoft ISA 2006	1
Disclaimer	2
Table of Contents.....	3
1 Reader	4
2 Overview.....	4
3 Problem Description.....	4
4 Solution	4
5 Technical Concept	5
5.1 General overview	5
5.2 Microsoft ISA 2006 prerequisites	5
5.3 IDENTIKEY Server Prerequisites	5
6 Microsoft ISA 2006	6
6.1 ISA 2006 configuration.....	6
7 IDENTIKEY Server.....	11
7.1 Policy configuration	11
7.2 Client configuration	14
8 Test VPN connection	16
9 About VASCO Data Security	19

1 Reader

This Document is a guideline for configuring the partner product with IDENTIKEY SERVER or Axsguard IDENTIFIER. For details about the setup and configuration of IDENTIKEY SERVER and Axsguard IDENTIFIER, we refer to the Installation and administration manuals of these products. Axsguard IDENTIFIER is the appliance based solution, running IDENTIKEY SERVER by default.

Within this document, VASCO Data Security, provides the reader guidelines for configuring the partner product with this specific configuration in combination with VASCO Server and Digipass. Any change in the concept might require a change in the configuration of the VASCO Server products.

The product name `IDENTIKEY SERVER` will be used throughout the document keeping in mind that this document applies as well to the Axsguard IDENTIFIER.

2 Overview

The purpose of this document is to demonstrate how to configure IDENTIKEY SERVER to work with Microsoft ISA 2006 (ISA) to secure the VPN connection with a One Time Password (OTP).

3 Problem Description

The basic working of ISA 2006 is based on authentication to an existing media (LDAP, Radius, ...). To use the IDENTIKEY SERVER with ISA 2006, some ISA 2006, RADIUS and IDENTIKEY SERVER settings need to be changed or added manually.

4 Solution

After configuring the IDENTIKEY SERVER and ISA 2006 in the right way, you eliminate the weakest link in any security infrastructure – the use of static passwords – that are easily stolen guessed, reused or shared.

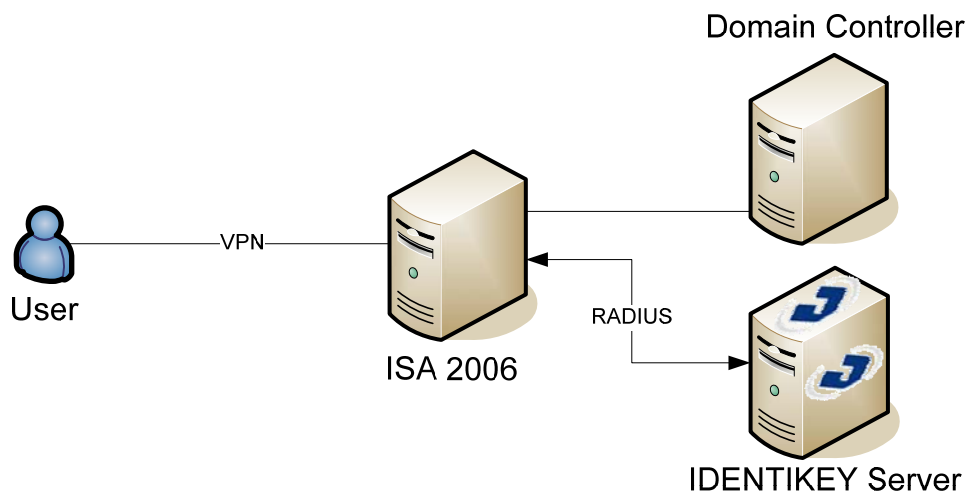


Figure 1: Solution

5 Technical Concept

5.1 General overview

The main goal of ISA 2006 is to perform authentication in a secure way to make a VPN connection. As ISA 2006 can do authentication to an external service with RADIUS, we will place the IDENTIKEY SERVER in the middle of this process to secure the authentication with our proven IDENTIKEY SERVER software.

5.2 Microsoft ISA 2006 prerequisites

Please make sure you have a working setup of a VPN connection in ISA 2006. It is very important this is working correctly before you start implementing the authentication to the IDENTIKEY SERVER.

5.3 IDENTIKEY Server Prerequisites

In this guide we assume you already have IDENTIKEY Server installed and working. If this is not the case, make sure you get it working before installing any other features.

6 Microsoft ISA 2006

6.1 ISA 2006 configuration.

Start the **ISA Server Management** tool.

In the left pane, select the **Virtual Private Networks (VPN)** option. In the right pane you will find all the necessary options to configure your VPN connections. We now will setup the **RADIUS** part of the authentication in ISA 2006.

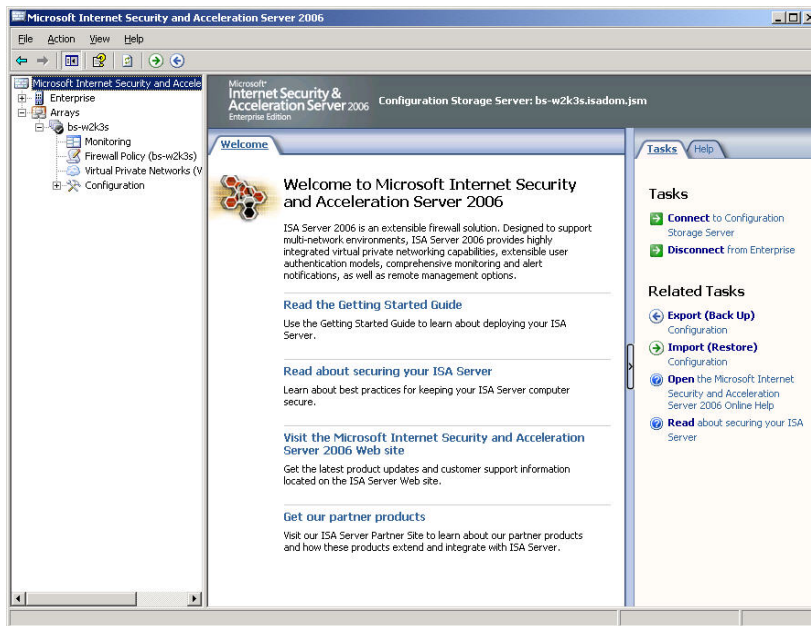


Figure 2: ISA 2006 welcome screen

In step 2 you will find the option **RADIUS server**. This is the only place where we will have to make some changes.

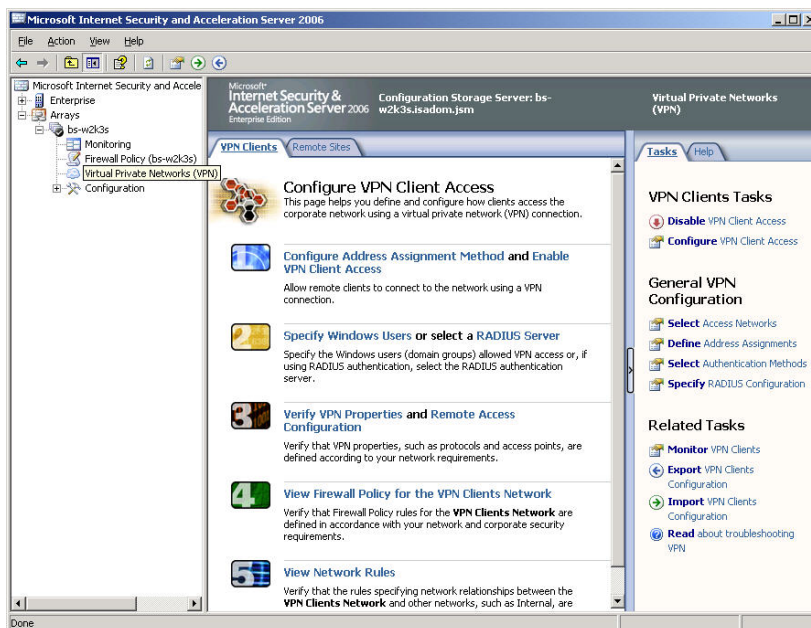


Figure 3: VPN configuration options

The authentication can be done directly to Active Directory or can be passed through to a RADIUS server. Depending on your previous situation, you may have to enable “**Use RADIUS for authentication**”.

Either way you will have to add or adjust the RADIUS server properties so click **RADIUS Servers...**

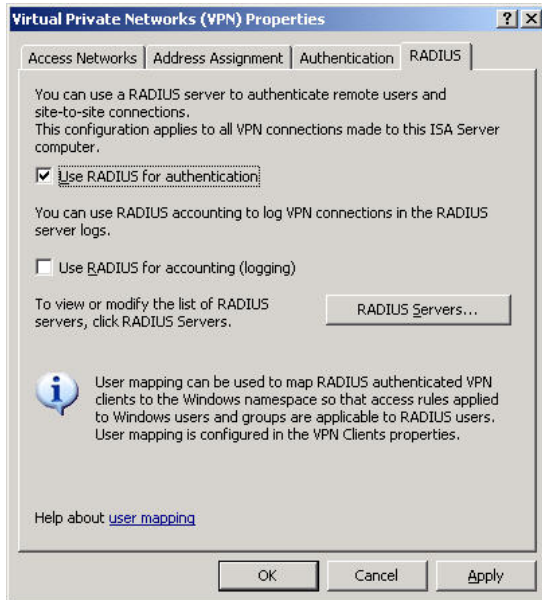


Figure 4: RADIUS Configuration (1)

In the next window you will get a list of RADIUS servers. If you have an existing RADIUS server, you will have to check that the previous server name or IP is different from the one where IDENTIKEY SERVER is installed. You can't have two servers with the same Server name or IP address. In this case you will have to **Edit...** the server properties. Otherwise you will have to **Add...** a new one.

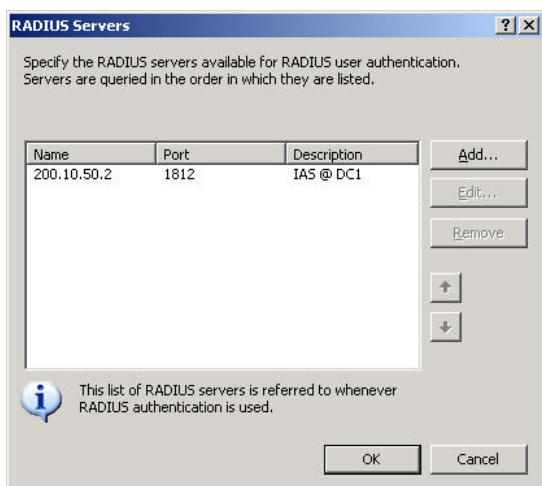


Figure 5: RADIUS Configuration (2)

At this point you will need the information where your IDENTIKEY SERVER is installed. Type in the **Server name** or IP address and give it a proper **Server description**. Set the **Authentication port** to the one used in IDENTIKEY SERVER, default is 1812. Then click the **Change...** button to create a **Shared secret**.



Figure 6: RADIUS Configuration (3)

Fill in a new RADIUS shared secret and confirm it in the second field. Click **Ok** to go back.

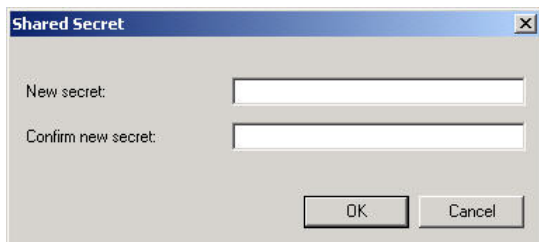


Figure 7: RADIUS Configuration (4)

This is the form as it should look like filled in completely. Click **OK** to continue.

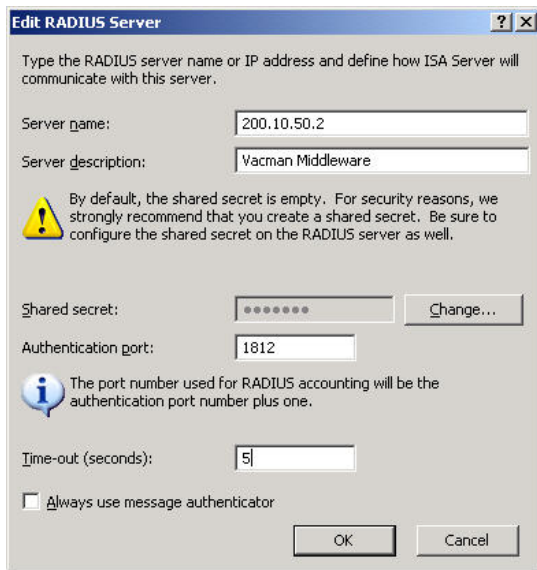


Figure 8: RADIUS Configuration (5)

In the overview you will see the newly added server. If you have more than one server in the list, make sure you move this server to the **top of the list** by using the two arrows beneath the Remove... button. Click **OK** to apply the changes.

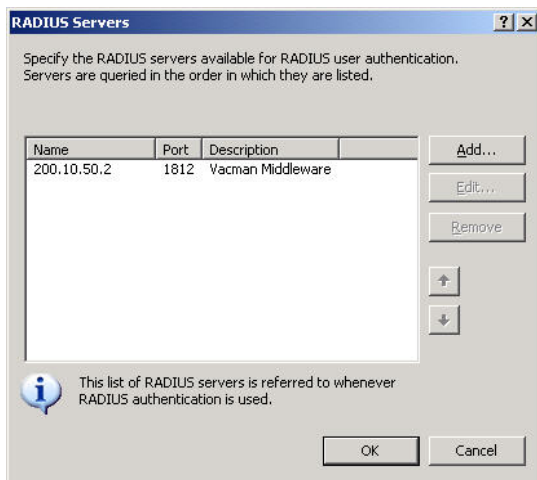


Figure 9: RADIUS Configuration (6)

You will receive a notice that the routing service may have to restart and that current VPN connections will be disconnected. Click **OK** to continue.

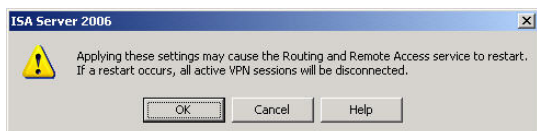


Figure 10: Apply changes

In the top of the screen you now will see two buttons. You can still discard any changes you made by pressing the **Discard** button. Otherwise click **Apply** to continue and then all changes will be saved.

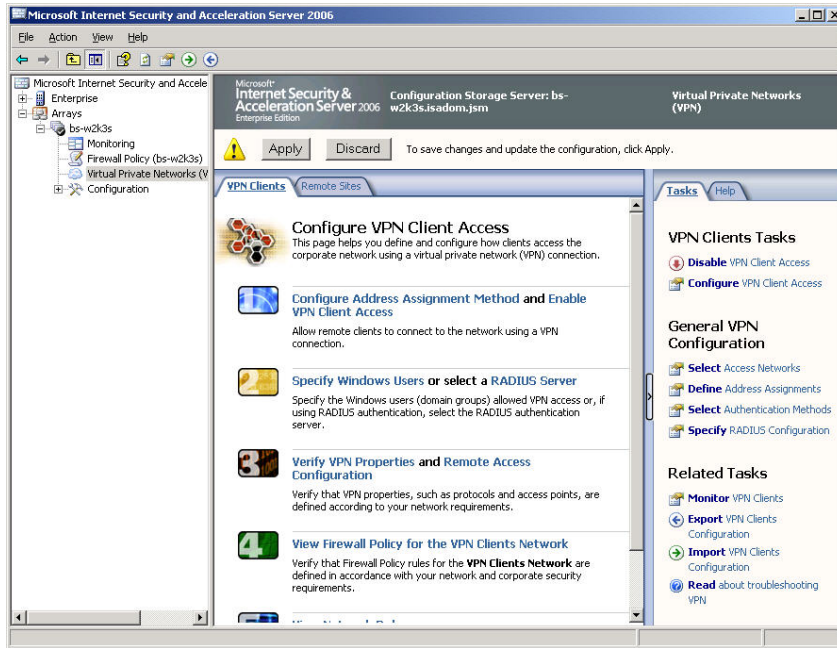


Figure 11: Apply or discard changes

You will receive a notification that all changes were correctly performed. Click **OK** to finish.

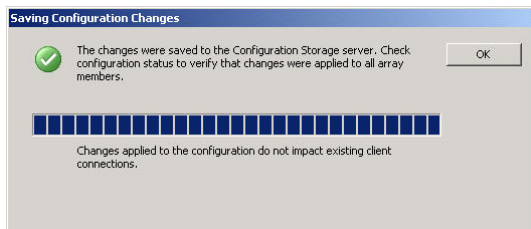


Figure 12: Saving configuration changes

7 IDENTIKEY Server

Go to the IDENTIKEY Server web administration page, and authenticate with an administrative account.

7.1 Policy configuration

To add a new policy, select **Policies ▶ Create**.

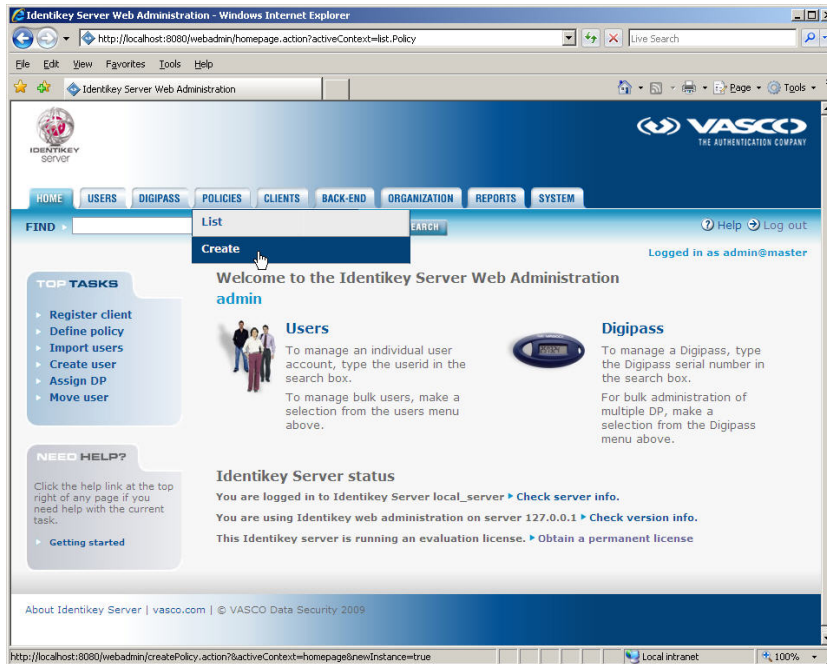


Figure 13: Policy configuration (1)

There are some policies available by default. You can also create new policies to suit your needs. Those can be independent policies or inherit their settings from default or other policies.

Fill in a **policy ID** and description. Choose the option most suitable in your situation. If you want the policy to inherit setting from another policy, choose the right policy in the **Inherits From** list. Otherwise leave this field to None.

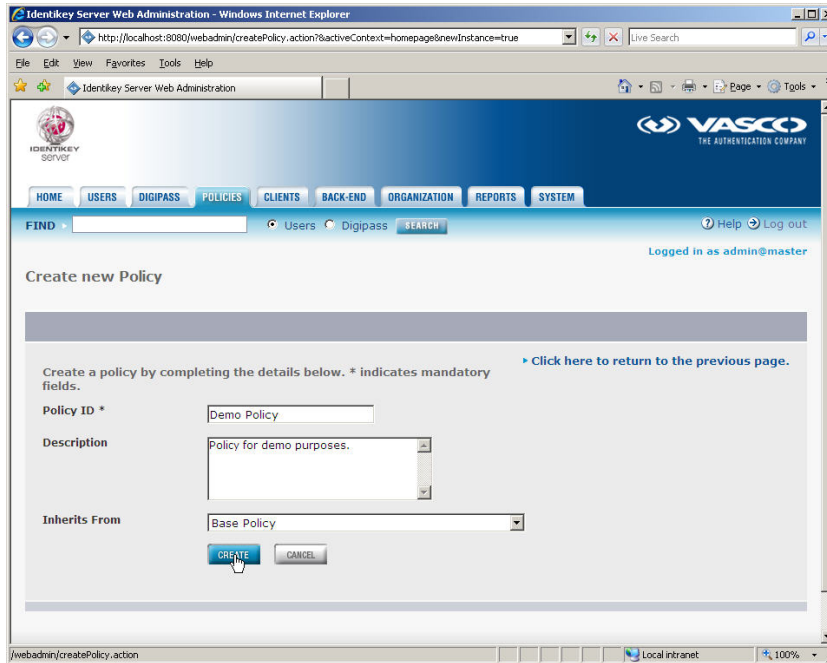


Figure 14: Policy configuration (2)

In the policy options configure it to use the right back-end server. This could be the local database, but also active directory or another radius server.

This is probably the same that was in your default client authentication options before you changed it. Or you use the local database, Windows or you go further to another radius server.

In our example we select our newly made **Demo Policy** and change it like this:

- *Local auth.:* Digipass/Password
- *Back-End Auth.:* Default (None)
- *Back-End Protocol:* Default (None)
- *Dynamic User Registration:* Default (No)
- *Password Autolearn:* Default (No)
- *Stored Password Proxy:* Default (No)
- *Windows Group Check:* Default (No Check)

After configuring this Policy, the authentication will happen locally in the IDENTIKEY Server. So user credentials are passed through to the IDENTIKEY Server, it will check these credentials to its local user database and will answer to the client with an Access-Accept or Access-Reject message.

In the Policy tab, click the **Edit** button, and change the **Local Authentication** to **Digipass/Password**.

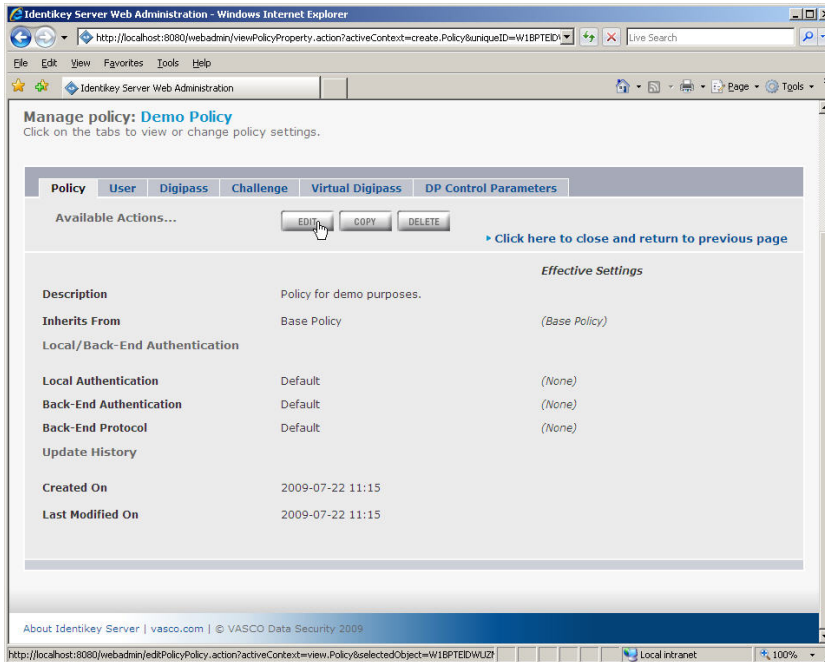


Figure 15: Policy configuration (3)

The user details can keep their default settings.

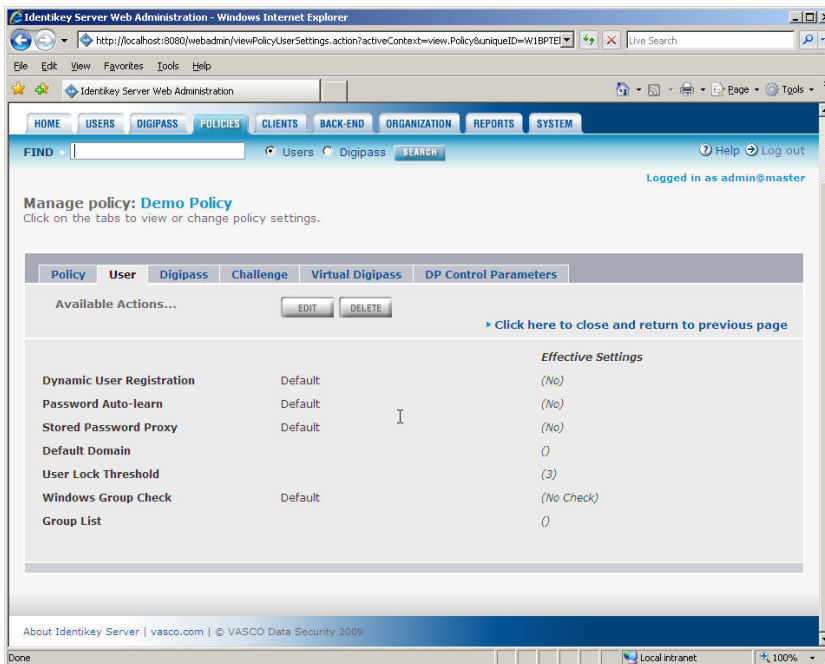


Figure 16: Policy configuration (4)

7.2 Client configuration

Now create a new component by right-clicking the Components and choose **New Component**.

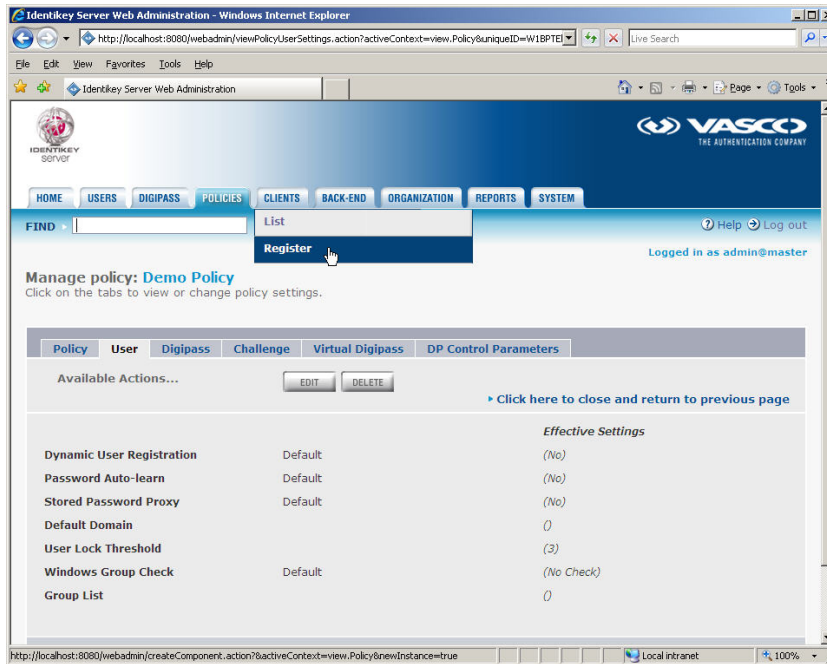


Figure 17: Client configuration (1)

As component type choose **RADIUS Client**. The location is the **IP address** of the client. In the policy field you should find your **newly created policy**. Fill in the **shared secret** you entered also in the client for the RADIUS options. In our example this was "vasco". Click **Create**.

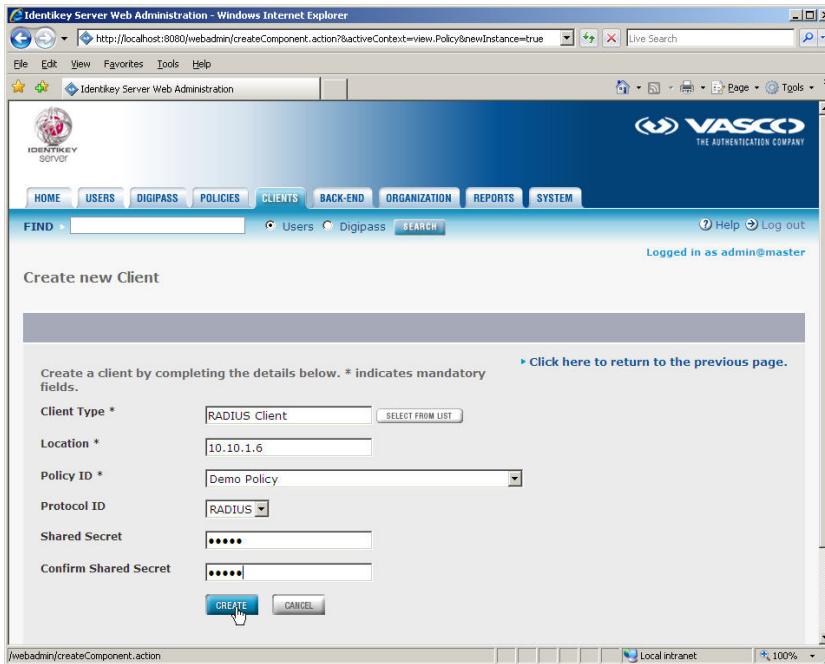


Figure 18: Client configuration (2)

Now the client and the IDENTIKEY Server are set up. We will now see if the configuration is working.

8 Test VPN connection

Create a new, or open an existing, VPN connection to the ISA 2006 Server. Click **Properties**.

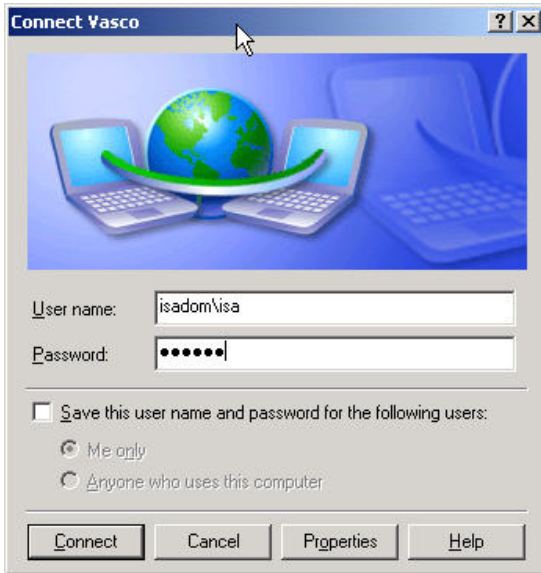


Figure 19: Making VPN connection

Select **Advanced (custom settings)**, and click the **Settings...** button.

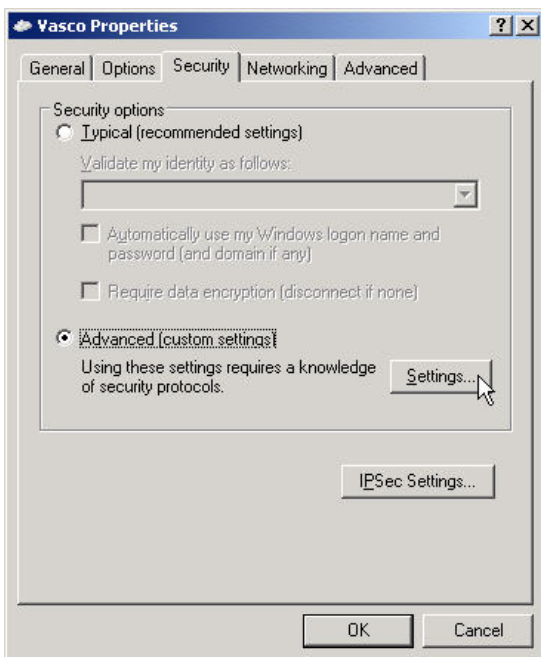


Figure 20: Connection settings

Choose **Optional encryption** (connect even if no encryption) in the Data encryption field at the top. Select the option **Allow these protocols** and make sure the following protocol is selected:

1. Unencrypted password (PAP)

These two protocols use no data encryption and are understood by IDENTIKEY SERVER. Click **OK** when done.

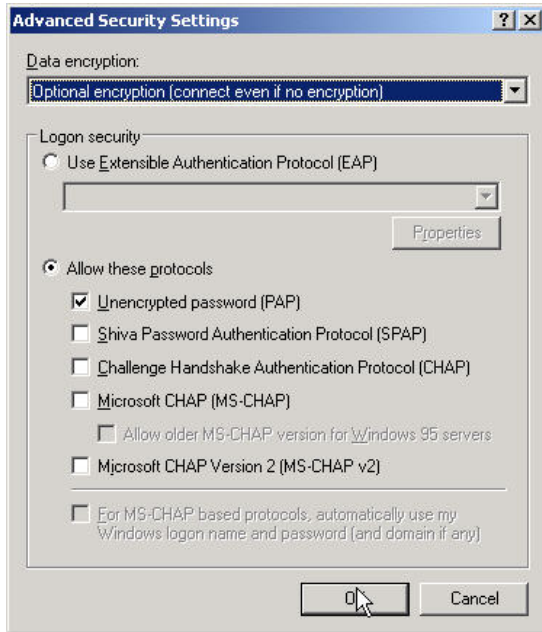


Figure 21: Advanced security options

The reason we will be using the PAP protocol is because hereby it is possible to challenge/response and complex login permutations. With CHAP / MSCHAP v1/2 / MPPE (MS Point to Point Encryption) the password and OTP are inseparably hashed. You will still be able to use an OTP in stead of a password, but not together. It will not work for example when the windows password has changed.

When you clicked OK you will receive a notification that PAP, SPAP and CHAP use no data encryption. Click **Yes** to continue and **OK** once again to close the next window.



Figure 22: Network connection warning

In the connection window, type your **User name** and Password. Only now, instead of your password you type in a **One Time Password (OTP)** and **Connect** to the ISA 2006 server.



Figure 23: Connection window

If everything went well, you should've established a VPN connection. If the connection isn't working you can always check the trace files for detailed debugging information.

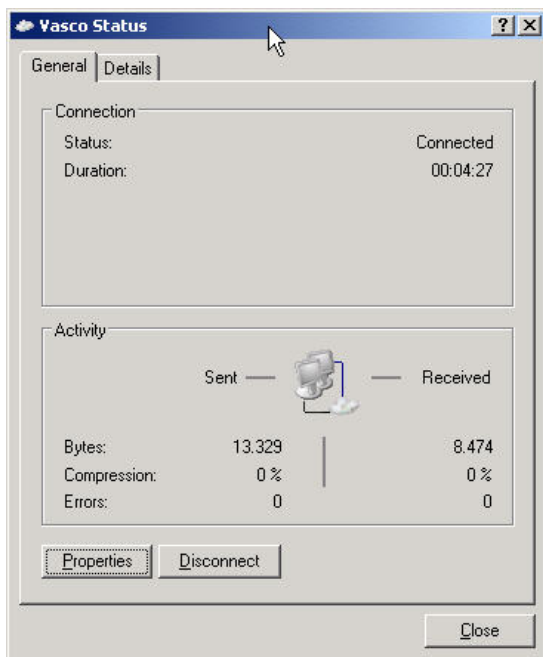


Figure 24: VPN connected

9 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO's User Authentication software is carried by the end user on its DIGIPASS products which are small "calculator" hardware devices, or in a software format on mobile phones, other portable devices, and PC's.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO's target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO's time-based system generates a "one-time" password that changes with every use, and is virtually impossible to hack or break.

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO's user authentication software is delivered via its DIGIPASS hardware and software security products. With over 25 million DIGIPASS products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 500 international financial institutions and almost 3000 blue-chip corporations and governments located in more than 100 countries.