DIGIPASS Authentication for Sonicwall Aventail SSL VPN

With VASCO IDENTIKEY Server 3.0

Integration Guideline
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 & VACMAN 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
© 2009 VASCO Data Security. All rights reserved.
7.3 DIGIPASS Assignment ................................................................. 33

8 MDC ........................................................................................................ 36
8.1 MDC Configuration ................................................................. 36

9 SonicWALL Aventail SSL/VPN test ......................................................... 39
9.1 Response Only ................................................................. 39
9.2 Challenge Response ................................................................. 41
9.3 Virtual DIGIPASS ................................................................. 44

10 IDENTIKEY features .......................................................................... 46
10.1 Installation .................................................................................. 46
10.1.1 Support for Windows 2003 and IIS6 .............................................. 46
10.1.2 Support for ODBC databases .................................................. 46
10.2 Deployment .................................................................................. 46
10.2.1 Dynamic User Registration (DUR) ........................................... 47
10.2.2 Autolearn Passwords .............................................................. 47
10.2.3 Stored Password Proxy .......................................................... 47
10.2.4 Authentication Methods ........................................................... 47
10.2.5 Policies .................................................................................. 47
10.2.6 DIGIPASS Self Assign .............................................................. 47
10.2.7 DIGIPASS Auto Assign .............................................................. 47
10.2.8 Grace Period ........................................................................ 47
10.2.9 Virtual DIGIPASS ................................................................. 47
10.3 Integration .................................................................................. 48
10.3.1 Remote Access Client Integration .......................................... 48
10.3.2 Backend Authentication .......................................................... 48
10.4 Administration ............................................................................ 48
10.4.1 Web Admin ........................................................................ 48
10.4.2 Request for OTP Web Site ..................................................... 49
10.4.3 User Self Management Web Site .......................................... 50
10.4.4 Delegated administration ....................................................... 50
1 Overview

SonicWall is a strong leader in secure, easy to configure and affordable SSL-VPN clientless remote access. This addresses all companies going from the SMB (Small and Medium Businesses) to the Enterprise space.

Vasco Data Security has a long history with delivering strong authentication through the DIGIPASS family that delivers the comfort of using One Time Passwords (OTP’s).

IDENTIKEY combined with SonicWALL Aventail SSL-VPN is the result of the open market approach delivered through IDENTIKEY technology.

IDENTIKEY and SonicWALL gives users the possibility to utilize the strength of the VASCO DIGIPASS family concept (One Time Password login as Time Based Response Only or Challenge/Response) for easy and secure clientless SSL-VPN remote access (everywhere and every time).

The purpose of this document is to demonstrate how to configure IDENTIKEY 3.0 to integrate with SonicWall Aventail to provide strong user authentication.

2 Problem Description

Since static password are generally known as non-secure and easy to compromise, the challenge was to introduce OTP’s (One Time Password) to the remote access market to strongly secure the corporate LAN or central resources. Additionally it would be nice to easily track and manage incoming users via the SonicWALL Aventail SSL-VPN.

Two-Factor authentication is an authentication method that requires two independent pieces of information to establish identity and privileges. Two-factor authentication is stronger and more rigorous than traditional password authentication that only requires one factor (the user’s password). For this reason SonicWALL Partners with VASCO to provide strong two-factor user authentication.

The following pages present how to solve these issues via a quick and easy configuration on both the SonicWALL Aventail SSL-VPN and the IDENTIKEY.

3 Solution

3.1 Overview

The basic working of the Sonicwall Aventail is based on authentication to an existing media (LDAP, RADIUS, local authentication …). To use the IDENTIKEY with SonicWALL Aventail, the external authentication settings need to be changed or added manually.

After configuring IDENTIKEY and the Sonicwall SSL VPN 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.

3.2 Benefits

Two-factor authentication offers the following benefits in combination with SonicWALL Aventail SSL-VPN:
• Greatly enhances security by requiring two independent pieces of information for authentication.

• Reduces the risk posed by weak user passwords that are easily cracked.

• Minimizes the time administrators spend training and supporting users by providing a strong authentication process that is simple, intuitive and automated.

3.3 How does two-factor authentication work?

Two-factor authentication requires the use of a third-party authentication service. The authentication service consists of two components:

• An authentication server on which the administrator configures the user names, assigns tokens, and manages authentication-related tasks, like VASCO IDENTIKEY.

• Tokens that the administrator gives to the user which displays One Time Passwords (OTP), like IDENTIKEY.

With two-factor authentication, users must enter a valid OTP to gain access. An OTP consists of the following:

• The user’s personal identification number (PIN) or static password

• A One Time Password.

Users receive the temporary token codes from their VASCO DIGIPASS. The DIGIPASS displays a new OTP every 32 seconds. (In case of an older DIGIPASS, the time was 36 seconds). When IDENTIKEY authenticate the user, it verifies that the OTP timestamp is valid in the current timeframe. If the user’s PIN is used, the IDENTIKEY will verify the PIN is correct, and the OTP is correct and current, the user is authenticated. If static password is used, the IDENTIKEY will forward the static password to the back-end (RADIUS or Domain Controller) to verify if the static password is correct. If the static password is correct, and the OTP is correct and current, the user is authenticated.

Because user authentication requires these two factors, the VASCO DIGIPASS solution offers a much stronger security than traditional passwords (single-factor authentication).
3.4 Network Diagram

Figure 1: SSL VPN with hardware DIGIPASS

Figure 2: SSL VPN with Virtual DIGIPASS
4 Technical Concept

4.1 General overview

The main goal of the Sonicwall Aventail is to perform authentication to secure all kinds of SSL VPN connections. As the Sonicwall Aventail can perform authentication to an external service using the RADIUS protocol, we will place the IDENTIKEY as back-end service for the Sonicwall Aventail appliance, to secure the authentication with our proven IDENTIKEY Server.

The users will now be authenticated first by IDENTIKEY Server that can be linked to the Active Directory in the back-end. So we will deploy the IDENTIKEY Server in between the Sonicwall Aventail and the Active Directory.

This means that the IDENTIKEY receives all authentication requests from SonicWALL Aventail SSL-VPN. The One Time Password (OTP) within the authentication requests will be verified by the IDENTIKEY. The IDENTIKEY will relay the static password to the back-end (RADIUS Server or Active Directory) for verification if required. After a successful verification, a RADIUS access-accept message will be sent to the SonicWALL Aventail SSL-VPN for the authentication part.

![Diagram](image)

Figure 3: General overview
4.2 Overview of SonicWALL Aventail Radius Authentication with IDENTIKEY

The following is a description on the RADIUS authentication sequence WITHOUT DIGIPASS assigned:

- Remote user initiates a connection to the SonicWALL Aventail SSL-VPN
- The SonicWALL Aventail gathers remote user’s ID and password and submits a RADIUS authentication requests to the IDENTIKEY
- IDENTIKEY performs verification (If back-end is required, static password will be sent to the back-end for verification) and answers to SonicWALL Aventail SSL-VPN with an access-accept or access-reject message.
- SonicWALL Aventail then provides access to the authenticated user’s individual Portal on the SonicWALL Aventail SSL-VPN where the protected resources can be accessed.

The following is a description on the RADIUS authentication sequence WITH a hardware DIGIPASS Assigned for Response Only Application:

- Remote user initiates a connection to the SonicWALL Aventail SSL-VPN
- The SonicWALL Aventail gathers remote user’s ID and password and submits a RADIUS authentication requests to the IDENTIKEY.
- IDENTIKEY performs OTP verification (If back-end is required, the static password will be forwarded to the back-end for verification) and answers to SonicWALL Aventail SSL-VPN with an access-accept or access-reject message.
- SonicWALL Aventail SSL-VPN then provides access to the authenticated user’s individual Portal on the SonicWALL Aventail SSL-VPN where the protected resources can be accessed.

The following is a description on the RADIUS authentication sequence WITH a hardware DIGIPASS Assigned for Challenge Response Application:

- Remote user initiates a connection to the SonicWALL Aventail SSL-VPN
- For the password field, the user will enter the (static password / keyword / PasswordKeyword / KeywordPassword) depending on the policy
- The SonicWALL Aventail gathers remote user’s ID and password and submits a RADIUS authentication requests to the IDENTIKEY.
- The IDENTIKEY will recognize that this is a request for challenge and generate a challenge and return back to SonicWALL Aventail.
- User will based on the generated challenge and enter the challenge onto the PIN protected DIGIPASS to generate an OTP
The SonicWALL Aventail gathers remote user’s ID and password and submits a RADIUS authentication requests to the IDENTIKEY.

IDENTIKEY performs OTP verification (If back-end is required, the static password will be forwarded to the back-end for verification) and answers to SonicWALL Aventail SSL-VPN with an access-accept or access-reject message.

SonicWALL Aventail SSL-VPN then provides access to the authenticated user’s individual Portal on the SonicWALL Aventail SSL-VPN where the protected resources can be accessed.

The following is a description on the RADIUS authentication sequence WITH a virtual DIGIPASS assigned:

- Remote user initiates a connection to the SonicWALL Aventail SSL-VPN.
- The SonicWALL Aventail gathers remote user’s ID and password and submits a RADIUS authentication requests to the IDENTIKEY.
- For the password field, the user will enter the (static password / keyword / PasswordKeyword / KeywordPassword) depending on the virtual DIGIPASS request method.
- The IDENTIKEY will check on the user record if the user is assigned with a virtual DIGIPASS. The IDENTIKEY will generate an OTP and forward to the SMS gateway for delivery of OTP to the user’s mobile via text message.
- The user will be directed into another page in the SonicWALL Aventail SSL VPN to enter the OTP received.
- Upon receiving the text message, the user will enter the OTP and login to the SonicWALL Aventail SSL-VPN.
- IDENTIKEY performs OTP verification (If back-end is required, the static password will be forwarded to the back-end for verification) and answers to SonicWALL Aventail SSL-VPN with an access-accept or access-reject message.
- SonicWALL Aventail SSL-VPN then provides access to the authenticated user’s individual Portal on the SonicWALL Aventail SSL-VPN where the protected resources can be accessed.

4.3 Sonicwall Aventail Prerequisites

Please make sure you have a working setup of the Sonicwall Aventail. It is very important that this is working correctly before you start implementing the authentication to the IDENTIKEY.

4.4 IDENTIKEY Server Prerequisites

In this guide we assume you already have the IDENTIKEY installed and working. If this is not the case, make sure you get IDENTIKEY working before installing any other features. Please refer to the IDENTIKEY Server Installation Guide as well as the IDENTIKEY Server Administration Guide for the setting up of IDENTIKEY Server.
4.5 SMS Gateway Prerequisites
If Virtual DIGIPASS is used, we assume that the SMS Gateway can support HTTP/HTTPS method and has been set up and running.

4.6 Active Directory Prerequisites
We assume that the Active Directory has already been set up. The active directory will be used as a back-end authentication for users’ static passwords. We assume that user account has already been created in the Active Directory.

5 SonicWALL Aventail

5.1 SonicWALL Aventail Configuration

5.1.1 Login to the SSL-VPN
By default the webconfig is reachable by following URL:

https://<IP_OR_NAME_SonicWALL_Aventail>:8443

In our case this becomes: https://192.168.88.144:8443

![Figure 4: Sonicwall Aventail Configuration (1)](image)

5.1.2 Configure Radius Server
First, we need to configure the radius server in the Sonicwall Aventail. From the main navigation menu on the AMC, click on Authentication Servers, and then click New to create a new authentication server.
Figure 5: Sonicwall Aventail configuration (2)

In the user store area, select Radius authentication and under Credential Type, select Username/Password. Click Continue to proceed.

Figure 6: Sonicwall Aventail configuration (3)

In the Name box, enter a name for the authentication server. In the Primary Radius Server, enter the IP Address and specify a port number as a colon-delimited suffix. (For example, 192.168.88.90:1812). If required, enter the IP Address of the secondary IDENTIKEY server in the Secondary Radius Server field. Enter the share secret that is used to secure communication with IDENTIKEY and click Save.
Figure 7: Sonicwall Aventail Configuration (4)

Click on **Pending changes** and **Apply** to apply the changes made.

Figure 8: Sonicwall Aventail Configuration (5)
5.1.3 Create Realm

From the main navigation menu, click Realms. Click New Realm to configure a new realm.

Click on New Realm to create to configure a new realm. In the Name text box, provide a meaning name for the Realm for users to select when logging in to the VPN. In the status field, enable the Realm by checking on the Enabled radio button. Select the VASCO as the authentication server that will be used to verify a user’s identity.
Click Finish and apply to complete the configuration and apply the settings onto the SonicWALL Aventail SSL-VPN.
6 IDENTIKEY Configuration

6.1 Login to the IDENTIKEY Web Console

Log in to the IDENTIKEY Server by going to the URL: http://IDENTIKEY_server_IP:8080/webadmin. For this demo, I will login to http://192.168.88.190:8080/webadmin.

![Login to IDENTIKEY Web Console](image)

*Figure 12: IDENTIKEY POLICY Configuration (1)*
6.2 Policy configuration

Create a new policy for users who will be authenticated via the SonicWALL Aventail. Go to the Policy Tab and select Create.

There are a few 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 name and description and select if this policy is going to inherit any settings from any existing policy and click Create. In this example, I will create a policy name called SonicWALL Aventail that will be referred to if the users are logging in to the network via SonicWALL Aventail SSL VPN. This policy will inherit default settings from the predefined policy IDENTIKEY Windows Password Replacement. For more information about the predefined policy and creation of policies, please refer to the IDENTIKEY Administrator Reference Guide.
In the **policy properties**, several settings can be configured. For example, whether if a back-end server will be used? This could be the local database, but also Windows (Active Directory) or another radius server (RADIUS). The policy configured below is for demonstrative purpose. For a more detailed explanation on configuring the policies, please refer to IDENTIKEY Product Guide and IDENTIKEY Server Administrator Reference.

For this example, we will set up for the IDENTIKEY to authenticate the users first and if needed, the Active Directory or Radius server will authenticate the static password. Since we have a Domain Controller in the back-end, we need to set the following parameters.

- **Policy tab**
  - Local auth : DIGIPASS/Password
  - Back-End Auth : If Needed
  - Back-End Protocol : Windows

By default, the inherit settings from IDENTIKEY Windows Password Replacement set the Backend Protocol as None. This parameter need to be changed to Windows. Click on **Edit** to change the settings.
Figure 15: IDENTIKEY POLICY Configuration (4)

In the backend Protocol field, click on the "Select From List" button and in the subsequent pop up, select Windows in the drag down menu. Click "OK" and "Save" to apply the settings.

Figure 16: IDENTIKEY POLICY Configuration (5)
In IDENTIKEY Server, DIGIPASS user accounts are identified by User ID and Domain. If users do not specify a domain in the login screen, it will default to master domain **IF** the domain value is not specified in the policy. Else, users will be associated to the domain specified in the policy. In this example, my domain has been set to VDSAPLAB.LOCAL. So user who log in to the SonicWALL Aventail SSL VPN specifying only the User ID will automatically be associated to **VDSAPLAB.LOCAL** domain.

Click on the user Tab in the main policy page. Click on **“Edit”** to configure the parameter for this setting.

- **User tab**
  - Dynamic User Registration : Yes
  - Password Autolearn : Yes
  - Stored Password Proxy : Yes
  - Default Domain : VDSAPLAB.LOCAL*
  - User lockout : 3
  - Windows Group Check : No Check

![Figure 17: IDENTIKEY POLICY Configuration (6)](image)

Provide the domain in the **“Default Domain”** field. In the **“Windows Group Check”** section, set to **“No Check”** and click **“Save”** to apply the settings.
Figure 18: IDENTIKEY POLICY Configuration (7)

- DIGIPASS tab
  - Assignment Mode: Neither
  - Search upwards in Org Hierarchy: No

*Assuming all DIGIPASS is stored in the VDSAPLAB domain and manually assigned by administrator.

Figure 19: IDENTIKEY POLICY Configuration (8)
The challenge tab is optional and is for users who held DIGIPASS that support **Challenge/Response**. SonicWALL Aventail SSL VPN can support a 2-Step Challenge/Response.

Click on **“Edit”** to configure the parameter for **Challenge/Response**.

- Challenge tab
  - 2 Step Challenge / Response
    - Request Method  :  **KeywordPassword**
    - Request Keyword :  **sonic**

---

**Figure 20: IDENTIKEY POLICY Configuration (9)**
Under the 2-step Challenge/Response section, set the request method to “KeywordPassword” and Request method to “sonic”. Click Save to apply the settings.

Figure 21: IDENTIKEY POLICY Configuration (10)

There are four methods in which a user can request for OTP. In my demo, I am using KeywordPassword to request for an OTP and I set the keyword to be otp. Therefore, in order to request for a SMS, I will key in otpPassword in the password field assuming my static password is Password.

- Virtual DIGIPASS Tab
  - Primary DIGIPASS
    - Request Method : keywordPassword
    - Request Keyword : otp

Click on Edit on the Virtual DIGIPASS Tab to configure the parameter.
In the Primary Virtual DIGIPASS section, set the Request method to **KeywordPassword** and the Request Keyword to “otp”. Click Save to apply the settings.
6.3 Component configuration

Create a new radius client component. Go to the **Clients** Tab in the home page and select **Register**.

Click on “**Select From List**” button and pop up menu will appear. Select Radius Client and click OK. Enter the IP Address of the SonicWALL Aventail in the location, select policy **SonicWALL Aventail** (created from the previous step) and enter the **share secret** to secure the communication between SonicWALL Aventail and IDENTIKEY.

**Figure 24: IDENTIKEY COMPONENT configuration (1)**

**Figure 25: IDENTIKEY COMPONENT Configuration (2)**
7 User configuration

7.1 User Creation

Create users to be authenticated by the IDENTIKEY when they are logging in to the SonicWALL Aventail SSL VPN. Users can be created via 4 different ways. The administrator can either manually add in the user via the Web configuration, imported into IDENTIKEY database, dynamic user registration or through the self registration web portal provided during IDENTIKEY installation. For this example, we will add in the user manually in the IDENTIKEY. For more information on how to add in users, please refer to the IDENTIKEY Product Guide and IDENTIKEY Administrator Reference.

On the Home page, click on the Users tab and select Create.

![Figure 26: IDENTIKEY USER Creation (1)](image)

In the subsequent page, enter the particulars of the users. For this example, my user ID will be demo1 and the domain VDSAPLAB.LOCAL. Click Create to apply settings.
The user will now show up in the Users list. At this point it will be exactly the same as when Dynamic User Registration (DUR) was enabled.
Click on the user **Demo1** which was created to display the user properties. On the User Account tab you should be able to see the status of the user accounts, whether if the account is enabled, whether if local or backend authentication is set. Click on the Info Tab to edit the particulars of the users.

Figure 29: IDENTIKEY USER Creation (4)

For users who are using virtual DIGIPASS, we need to enter the user’s phone number in their record. Click on **Edit** to make changes to the user record.

Figure 30: IDENTIKEY USER Creation (5)
Enter the user’s particulars and in the mobile phone field, enter the country code followed by the mobile phone number. Click **Save** to apply the changes.

Figure 31: IDENTIKEY USER Creation (6)

7.2 Import DIGIPASS

Move the mouse over to **DIGIPASS** Tab and select **Import**.

Figure 32: IDENTIKEY DIGIPASS Import (1)
Click on the **browse** button to select the DPX file to import and enter the 32 digit **Transport key** and click **upload**.

**Figure 33: IDENTIKEY DIGIPASS Import (2)**

Select the applications to be imported into the IDENTIKEY. Click **Next** to continue.

**Figure 34: IDENTIKEY DIGIPASS Import (3)**
Select the domain which the DIGIPASS will be imported to and click Import.

**Figure 35: IDENTIKEY DIGIPASS Import (4)**

Click Finish to complete the Import process.

**Figure 36: IDENTIKEY DIGIPASS Import (5)**
7.3 DIGIPASS Assignment

There are two possible ways to assign a DIGIPASS to a user. You can search for a DIGIPASS and assign it to a user or you can search for a user and assign it to a DIGIPASS. You can see the difference in the following two figures. For demonstration purpose, I will select a user and find all available DIGIPASS that can be assigned to this user. For more information on assigning DIGIPASS, please refer to the IDENTIKEY Administrator Reference.

Move the mouse over to the Users tab and select List to display all users.

![Figure 37: IDENTIKEY DIGIPASS Assignment (1)](image1)

A list of users that are in the IDENTIKEY will be displayed. Select the user to be assigned with a DIGIPASS. In this example, I will select user dem01.

![Figure 38: IDENTIKEY DIGIPASS Assignment (2)](image2)
Click on the **Assigned DIGIPASS Tab**. If there are no DIGIPASS assigned to the user, click on the **Assign** button.

![Figure 39: IDENTIKEY DIGIPASS assignment (3)](image)

On the subsequent page, navigate to the bottom of the page and in the “**On clicking Next**” section, select **“Search Now To Select DIGIPASS To Assign”**.

![Figure 40: IDENTIKEY DIGIPASS assignment (4)](image)
A list of available DIGIPASS will be presented. Select one of the appropriate available DIGIPASS and click “Next”.

Figure 41: IDENTIKEY DIGIPASS assignment (5)

Provide the number of grace period for this user. Default setting is 7 days. Click Assign.

Figure 42: IDENTIKEY DIGIPASS assignment (6)
Review the assignment and click **Finish**.

![IDENTIKEY DIGIPASS assignment](image)

**Figure 43: IDENTIKEY DIGIPASS assignment (7)**

## 8 MDC

### 8.1 MDC Configuration

This component is optional and is required only when Virtual DIGIPASS is used. The Message Delivery Component (MDC) interfaces with a gateway service to send a One Time Password to a User’s mobile phone. The MDC acts as a service, accepting messages from the IDENTIKEY server, which are then forwarded to a text message gateway via the HTTP/HTTPS protocol.

In the IDENTIKEY server, open up the Virtual DIGIPASS Message Delivery Component. In the General Tab, it will display a list of information such as the location of the IDENTIKEY server, the port setting, SMS Gateway credentials for example.

In the Message Delivery Component section, configure the Server IP and the port to connect to. In the HTTP Gateway Account section, enter a valid user ID and Password that is being used to log in to the SMS Gateway.
In the gateway settings tab, configure the information of the SMS Gateway. In the HTTP Gateway Name, enter an appropriate name to identify the SMS Gateway the MDC is connecting to.

Check on **Advance Settings**. Select whether to use HTTP or HTTPS protocol when connecting to the SMS Gateway. In the **Address** field, enter the URL to connect to the SMS Gateway. Enter the **port** number that the SMS Gateway is listening on and if necessary, provide the information where the certificate file for the IDENTIKEY server is stored.

In the **HTTP/HTTPS Query**, enter the query string format which the SMS Gateway is expecting and define whether if it is HTTP POST or HTTP GET.
Click on the Gateway Result Tab. Select SUCCESS Message and click **Edit**.

**Figure 45: MDC Configuration (3)**

Provide a matching pattern return code status that the MDC expect the SMS Gateway to return if the text message has been successfully delivered.

**Figure 46: MDC Configuration (4)**
9 SonicWALL Aventail SSL/VPN test

9.1 Response Only
To start the test for Response Only application, browse to the public IP address or hostname of the SonicWALL Aventail device. For Example, https://IP_Address_SonicWALL_Aventail

Select Vasco as the Auth method and click Next.

![Image of SSL-VPN Test]

Figure 47: SSL-VPN Test (1)

Enter the user’s credential to log in to the VPN. Enter the user ID in the username field. In the password field, enter the static password followed by the OTP generated from the DIGIPASS. For example if my password is abc123 and my OTP generated is 987654, then I should key in “abc123987654” in my password field.
If my login is successful, I should be prompted to install Aventail Access Manager to set up the SSL VPN tunnel.

Figure 48: SSL-VPN Test (2)

Figure 49: SSL-VPN Test (3)
When my SSL VPN has been setup correctly, I should be able to see my web portal.

![SSL VPN Test Image](image)

**Figure 50: SSL-VPN Test (4)**

### 9.2 Challenge Response

To start the test for **Challenge/Response** application, browse to the public IP address or hostname of the SonicWALL Aventail device. For Example, [https://IP_Address_Of_SonicWALL_Aventail](https://IP_Address_Of_SonicWALL_Aventail)

Select **Vasco** as the Auth method and click **Next**.
Enter the user ID in the Username field. In the password field, enter the method which was predefined to request for a challenge. For example, in my demo, I configured previously my request method is **KeywordPassword** and Request keyword is **sonic**. So I should enter demo1 as my user requesting for the challenge, and **sonicabc123** to request for a challenge. Click Log In.

The challenge will be displayed in the next screen. Key in the challenge displayed into the PIN protected DIGIPASS to retrieve the OTP. In this case, I will enter the challenge 9566 into my DP300 and click OK.
If my login is successful, I should be prompted to install Aventail Access Manager to set up the SSL VPN tunnel.

When my SSL VPN has been setup correctly, I should be able to see my web portal.
9.3 Virtual DIGIPASS

To start the test for Virtual DIGIPASS application, browse to the public IP address or hostname of the SonicWALL Aventail device.

Select Vasco as the Auth method and click Next.

Figure 56: SSL-VPN Test (9)

Enter the user ID into the username field. I previously configured the method to request for an OTP is KeywordPassword and my keyword is otp. In order to receive a SMS, key in the keyword (otp) follow by my password (abc123). Therefore, in my password field, I should key in otpabc123 to request for a sms.
Figure 57: SSL-VPN Test (10)

If the keyword is correct and the domain controller validated my password successfully, the IDENTIKEY will generate an OTP and send to the SMS gateway for delivery of SMS to my mobile. After I receive my SMS, I can use the OTP to log in. Enter the generated OTP in the "Enter One-Time Password" field and click OK.

![Figure 57: SSL-VPN Test (10)](image)

Figure 58: SSL-VPN Test (11)

If my login is successful, I should be prompted to install Aventail Access Manager to set up the SSL VPN tunnel.

![Figure 58: SSL-VPN Test (11)](image)

Figure 59: SSL-VPN Test (12)
When my SSL VPN has been setup correctly, I should be able to see my web portal.

10 IDENTIKEY features

10.1 Installation

The IDENTIKEY installation is very easy and straightforward. IDENTIKEY runs on Windows and Linux platforms, supports a variety of databases and uses an online registration. Different authentication methods allow a seamless integration into existing environments.

10.1.1 Support for Windows 2003 and IIS6

IDENTIKEY can be installed on Windows 2003 (32 or 64 bit) with Service pack 1 or above. Web modules exist for IIS 6 to protect Citrix Web Interface, Citrix Secure Gateway, Citrix Secure Access Manager (Form-based authentication), Citrix Access Gateway and Microsoft Outlook Web Access 2000 and 2003 (Basic Authentication and Form-Based Authentication).

10.1.2 Support for ODBC databases

Other ODBC compliant database can be used instead of the default PostgreSQL database. The supported database are MS SQL Server, Oracle, Sybase, DB2 and Postgres.

10.2 Deployment

Several IDENTIKEY features exist to facilitate deployment. Combining these features provides different deployment scenarios from manual to fully automatic.
10.2.1 Dynamic User Registration (DUR)
This feature allows IDENTIKEY to check a username and password not in the database with a back-end RADIUS server or a Windows domain controller and, if username and password are valid, to create the username in the IDENTIKEY database.

10.2.2 Autolearn Passwords
Saves administrators time and effort by allowing them to change a user’s password in one location only. If a user tries to log in with a password that does not match the password stored in the IDENTIKEY database, IDENTIKEY can verify it with the back-end RADIUS server or the Windows domain controller and, if correct, store it for future use.

10.2.3 Stored Password Proxy
Allows IDENTIKEY to save a user’s RADIUS server password or Windows domain controller password in the database (static password). User’s can then log in with only username and dynamic one-time password (OTP). If this feature is disabled, users must log in with username and static password immediately followed by the OTP.

10.2.4 Authentication Methods
Different authentication methods can be set on server level and on user level: local authentication (IDENTIKEY only), Back-End authentication (Windows or RADIUS). On top of that a combination of local and back-end can be configured. The additional parameters ‘always’, ‘if needed’ and ‘never’ offers you additional customization of the back-end authentication process.

The configuration of authentication methods is done within the policy (policies).

10.2.5 Policies
Policies specify various settings that affect the User authentication process. Each authentication request is handled according to a Policy that is identified by the applicable Component record. Components can be radius clients, authentication servers or Citrix web interfaces.

10.2.6 DIGIPASS Self Assign
Allows users to assign DIGIPASS to themselves by providing the serial number of the DIGIPASS, the static password and the OTP.

10.2.7 DIGIPASS Auto Assign
Allows automatic assignment of the first available DIGIPASS to a user on user creation.

10.2.8 Grace Period
Supplies a user with a certain amount of time (7 days by default) between assignment of a DIGIPASS and the user being required to log in using the OTP. The Grace Period will expire automatically on first successful use of the DIGIPASS.

10.2.9 Virtual DIGIPASS
Virtual DIGIPASS uses a text message to deliver a One Time Password to a User’s mobile phone. The User then logs in to the system using this One Time Password.

Primary Virtual DIGIPASS
A Primary Virtual DIGIPASS is handled similarly to a standard physical DIGIPASS. It is imported into the VACMAN Middleware database, assigned to a User, and treated by the IDENTIKEY database as any other kind of DIGIPASS.

**Backup Virtual DIGIPASS**

The Backup Virtual DIGIPASS feature simply allows a User to request an OTP to be sent to their mobile phone. It is not treated as a discrete object by IDENTIKEY, and is not assigned to Users, only enabled or disabled. It can be enabled for Users with another type of DIGIPASS already assigned, and used when the User does not have their DIGIPASS available.

### 10.3 Integration

#### 10.3.1 Remote Access Client Integration

IDENTIKEY Server supports RADIUS protocol (RFC 2865) for remote access authentication. The DIGIPASS packs include support for Citrix Web Interface, Outlook Web Access and IIS Basic authentication. IDENTIKEY Server also provides support for web applications through an SDK based on standard SOAP protocol.

#### 10.3.2 Backend Authentication

Back-End Authentication can be used for verification of users’ static password with another system. This could be a Windows or Radius server or custom Back-End application. For Wintel and Linux platforms, the back-end systems supported are RADIUS, Microsoft AD and Novell eDirectory using LDAP Protocol.

### 10.4 Administration

#### 10.4.1 Web Admin

Administration of the IDENTIKEY can be done via the web browser. Browse to the following url to administer the IDENTIKEY

http://ip_Address_Of_IDENTIKEY:8080/webadmin.
10.4.2 Request for OTP Web Site

A web site running on IIS has been developed to allow users to request for virtual DIGIPASS rather than from the login page.
10.4.3 User Self Management Web Site

A web site running on IIS has been developed to allow users to register themselves to the VM with their username and back-end (RADIUS or Windows) password, to do a DIGIPASS self assign, to update their back-end password stored in the IDENTIKEY database, to do a change PIN (Go-1/Go-3 DIGIPASS), to do a DIGIPASS test.

10.4.4 Delegated administration

Administration can be delegated by appointing different administrators per organizational unit (OU). These administrators can only see the DIGIPASS and users that were added to his OU.

10.4.5 Granular Access Rights

It is possible in VACMAN Middleware to setup different permission per user. This can be in function of a domain or an organizational unit. Administrators belonging to the Master Domain may be assigned administration privileges for all domains in the database, or just their own domain. Administrators belonging to any other Domain will have the assigned administration privileges for that Domain only.

It’s possible to set different operator access levels. E.g. An user can be created that only has the rights to unlock a DIGIPASS.
11 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.