



THE AUTHENTICATION COMPANY

DIGIPASS Authentication for GajShield GS Series

With Vasco VACMAN Middleware 3.0

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

© 2008 VASCO Data Security. All rights reserved.

Table of Contents

DIGIPASS Authentication for GajShield GS Series	1
Disclaimer	2
Table of Contents.....	3
1 Overview.....	5
2 Problem Description.....	5
3 Solution	5
3.1 VPN Client	5
4 Technical Concept	6
4.1 General overview	6
4.2 GajShield prerequisites	6
4.3 VACMAN Middleware Prerequisites	6
5 GajShield configuration.....	7
5.1 RADIUS Server	8
5.2 RADIUS Users.....	10
5.3 VPN Settings	12
5.4 Firewall Settings.....	13
6 VACMAN Middleware	14
6.1 Policy configuration	14
6.2 Component configuration.....	16
7 User configuration	17
7.1 ODBC installation	17
7.1.1 User creation	17
7.1.2 Import DIGIPASS.....	19
7.1.3 DIGIPASS Assignment.....	21
7.2 Active Directory installation	23
7.2.1 User creation.....	23

7.2.2	<i>Import DIGIPASS</i>	25
7.2.3	<i>DIGIPASS assignment</i>	27
8	GajShield VPN test	29
9	VACMAN Middleware features	31
9.1	Installation	31
9.1.1	<i>Support for Windows 2000, 2003, IIS5 and IIS6</i>	31
9.1.2	<i>Support for ODBC databases and Active Directory</i>	31
9.2	Deployment.....	31
9.2.1	<i>Dynamic User Registration (DUR)</i>	31
9.2.2	<i>Autolearn Passwords</i>	31
9.2.3	<i>Stored Password Proxy</i>	31
9.2.4	<i>Authentication Methods</i>	31
9.2.5	<i>Policies</i>	32
9.2.6	<i>DIGIPASS Self Assign</i>	32
9.2.7	<i>DIGIPASS Auto Assign</i>	32
9.2.8	<i>Grace Period</i>	32
9.2.9	<i>Virtual DIGIPASS</i>	32
9.3	Administration	33
9.3.1	<i>Active Directory Users and Computers Extensions</i>	33
9.3.2	<i>Administration MMC Interface</i>	33
9.3.3	<i>User Self Management Web Site</i>	34
9.3.4	<i>Delegated administration</i>	34
9.3.5	<i>Granular access rights</i>	34
10	About VASCO Data Security	35

1 Overview

The purpose of this document is to demonstrate how to use the GajShield GS Series in combination with a DIGIPASS. We will show you how to import a DPX file, how to assign a DIGIPASS to a user and show some administrative options.

2 Problem Description

The basic working of the GajShield is based on authentication to an existing media (LDAP, Radius, local authentication ...). To use the VACMAN Middleware with the GajShield, the authentication settings need to be changed.

3 Solution

After configuring VACMAN Middleware and the GajShield 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.

3.1 VPN Client

Users have the ability to run their corporate client/server applications from any location. Access can be filtered on Port, IP or IP range, giving administrators the ability to control application access on a user or group basis.

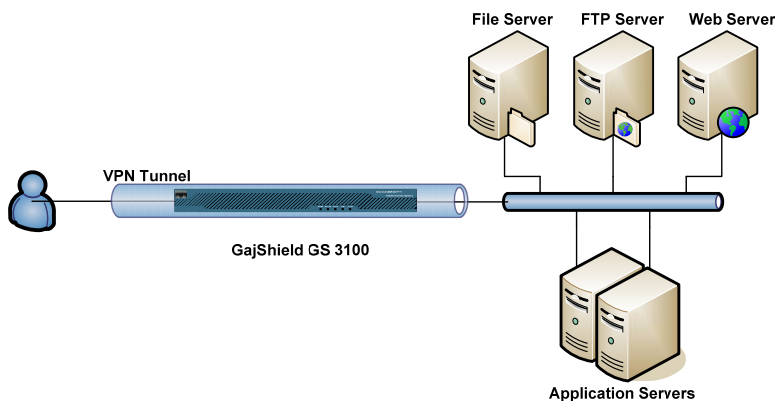


Figure 1: VPN Client

4 Technical Concept

4.1 General overview

The main goal of the GajShield is to perform authentication to secure all kind of VPN and firewall connections. As the GajShield can perform authentication to an external service using the RADIUS protocol, we will place the VACMAN Middleware as back-end service, to secure the authentication with our proven VACMAN Middleware software.

4.2 GajShield prerequisites

Please make sure you have a working setup of a GajShield GS Series device. It is very important this is working correctly before you start implementing the authentication to the VACMAN Middleware.

At this time this is a list of devices supported:

- GajShield GS 500A
- GajShield GS 1100
- GajShield GS 2100
- GajShield GS 3100
- GajShield GS 4100
- GajShield GS 5100
- GajShield GS 6100
- GajShield GS 7100
- GajShield GS 8100
- GajShield GS 400E
- GajShield GS 800E

The screenshots used in the rest of this document, are taken from a GajShield GS 3100.

4.3 VACMAN Middleware Prerequisites

In this guide we assume you already have VACMAN Middleware 3.0 (VM3.0) installed and working. If this is not the case, make sure you get VM working before installing any other features.

5 GajShield configuration

Go to the web administration page of the GajShield GS Series device. This is located at **https://<ip of GajShield>**. Enter the administrative username and password.

In our case this becomes: <https://192.168.2.180>.

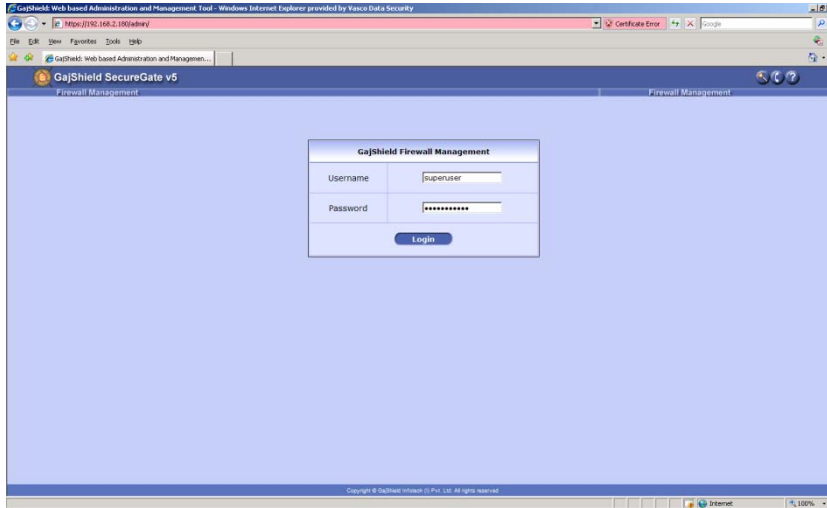


Figure 2: GajShield configuration

5.1 RADIUS Server

On the left menu, select **Firewall > Networks**. Make sure the **Hosts** tab is selected on the main screen and click on the  **button** on the right side of the screen to add a host.

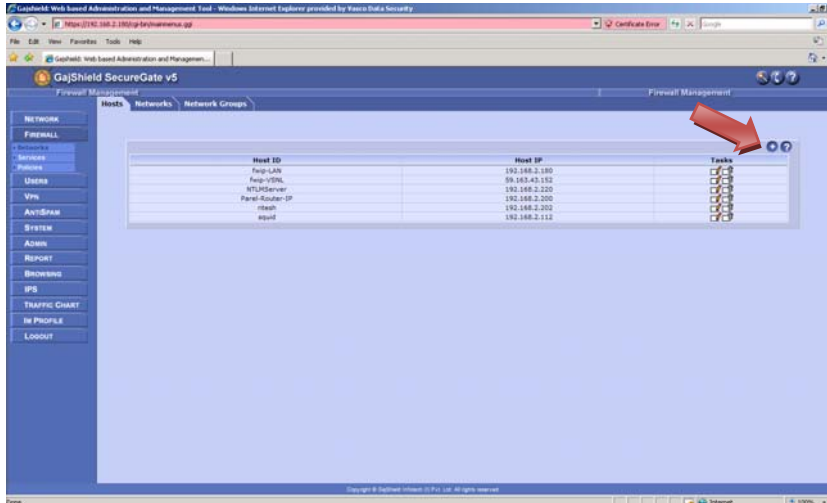


Figure 3: RADIUS Server (1)

Add the **Host ID** and the **Host IP** of the server that has the VACMAN Middleware installed. Click on **Add** to continue.

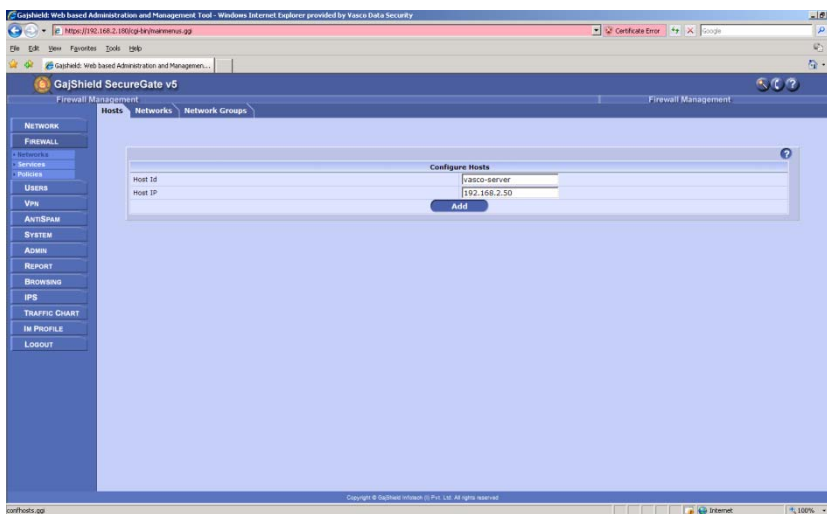


Figure 4: RADIUS Server (2)

After adding the host it will appear in the list as shown below.

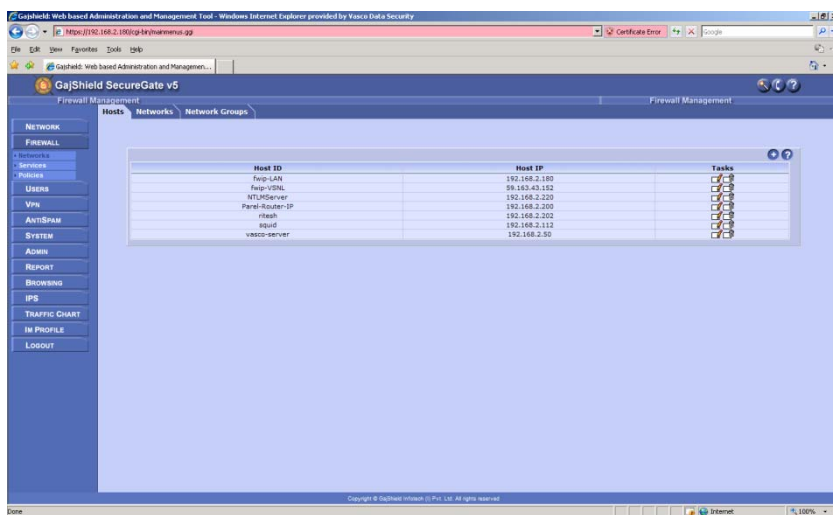


Figure 5: RADIUS Server (3)

5.2 RADIUS Users

Select the **Users** button on the left and make sure the **RADIUS** tab on the right is selected. Click on the button on the right side of the screen to add RADIUS users.

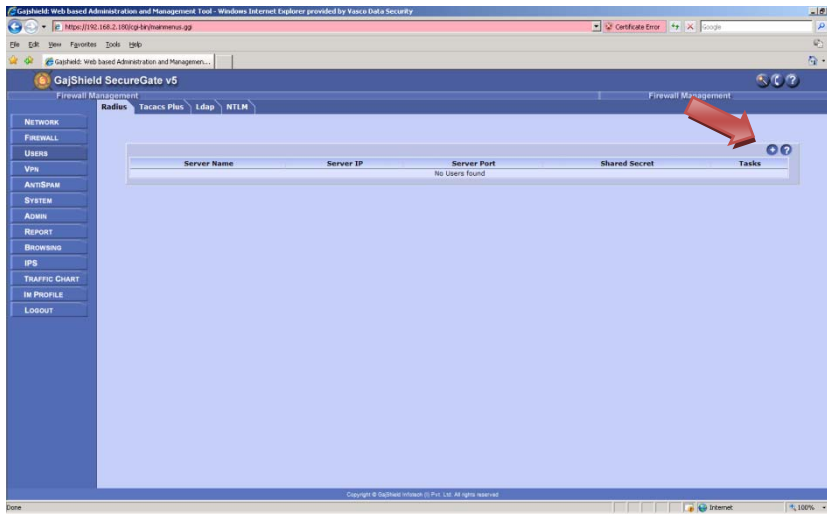


Figure 6: RADIUS Users (1)

Enter a RADIUS **Server Name**. Select the correct server from the **Server IP** that points to the VACMAN Middleware. Give in the **Server port** and the **Shared Secret** so it matches the settings from the VACMAN Middleware. Click the **Add** button to go on.

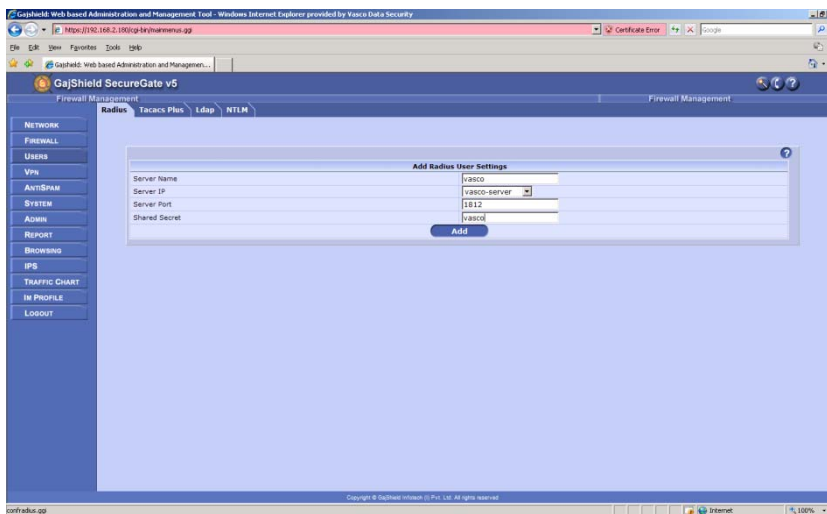


Figure 7: RADIUS Users (2)

After adding the RADIUS server it will appear in the list as shown below.

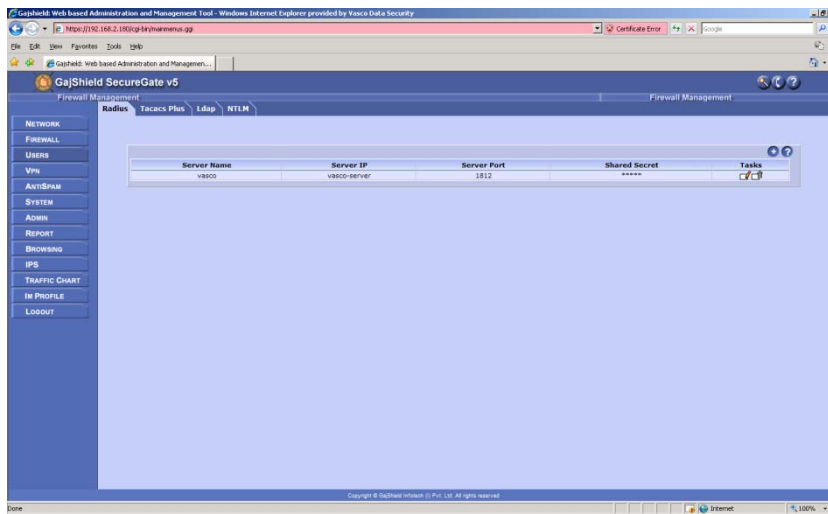


Figure 8: RADIUS Users (3)

5.3 VPN Settings

Now Select **VPN > IPsec** on the left menu and make sure the **Advanced Setup** Tab is selected.

Change the **XAUTH Authentication Scheme** to "radius".

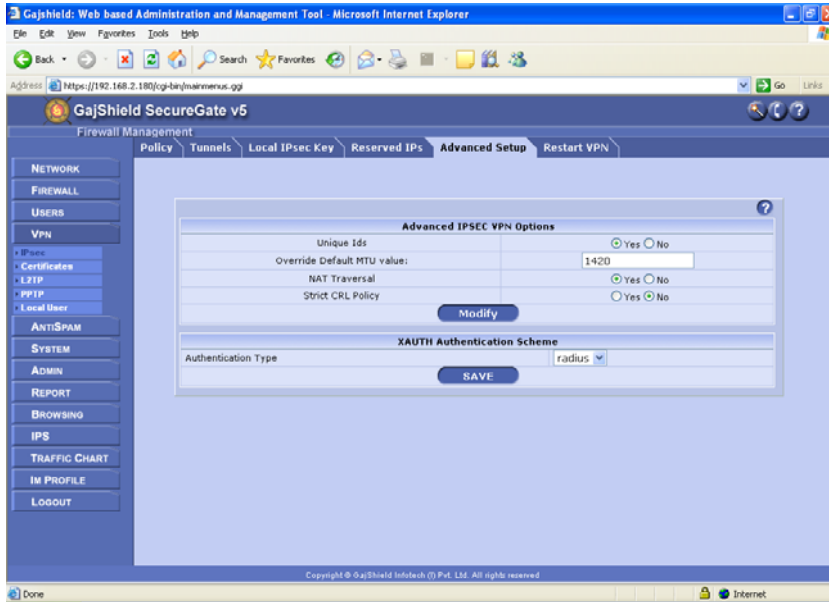


Figure 9: VPN Settings

5.4 Firewall Settings

Select **Firewall > Policies** on the left menu.

Add a rule here to enable communication between the GajShield device and the VACMAN Middleware over the RADIUS port.

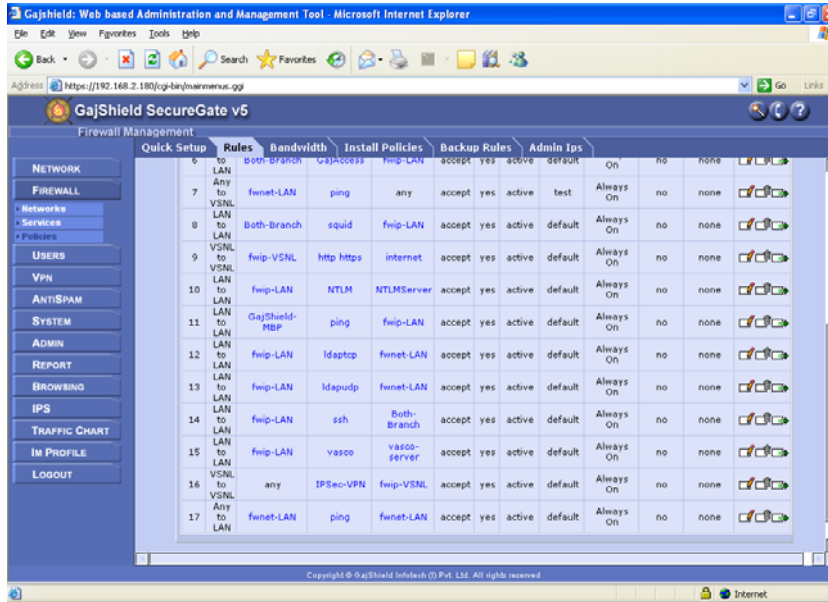


Figure 10: Firewall Settings

6 VACMAN Middleware

6.1 Policy configuration

Setting up the VM only requires you to set up a policy to go to the right back-end and to add an extra Radius component pointing to the ISA server.

To add a new policy, right-click Policies and choose **New Policy**.

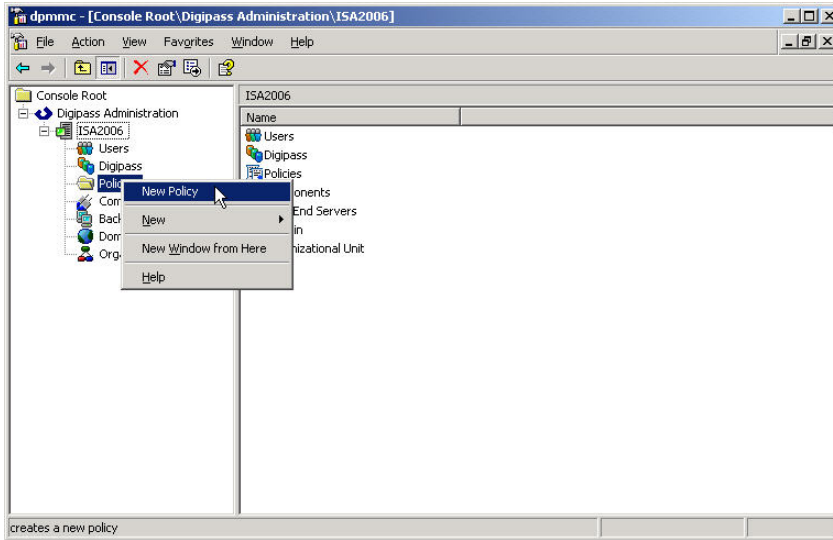


Figure 11: VM configuration (1)

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

Fill in a **policy name** and choose the **option** most suitable in your situation. If you want the policy to inherit setting from another policy, choose the inherit option. If you want to copy an existing policy, choose the copy option and if you want to make a new one, choose the create option.

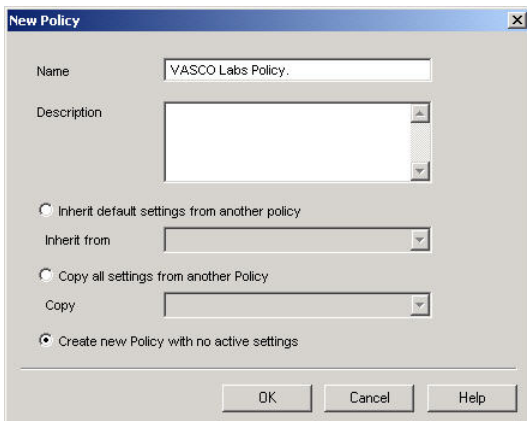


Figure 12: VM configuration (2)

We chose to create a new policy and specify all details about the authentication policy.

In the **policy properties** configure it to use the right back-end server. This could be the local database, but also Windows (Active Directory) or another radius server (RADIUS).

This could be the same authentication service as you were previously using in the ISA server.

- Main Settings tab
 - Local auth.: **Digipass/Password**
 - Back-End Auth.: **If Needed**
 - Back-End Protocol: **Windows**
- User Settings tab
 - Dynamic User Registration: **Yes**
 - Password Autolearn: **Yes**
 - Stored Password Proxy: **Yes**
 - Windows Group Check: **No Check**
- Challenge Settings tab
 - 2-Step Challenge Response: **None**
 - Primary Virtual DIGIPASS: **None**

After configuring this Policy, the authentication will happen, if needed (when it does not know the user locally), in the back-end to Active Directory. User credentials are passed through to the VM, it will check these credentials with the AD and will answer to the ISA server with an Access-Accept or Access-Reject RADIUS message.

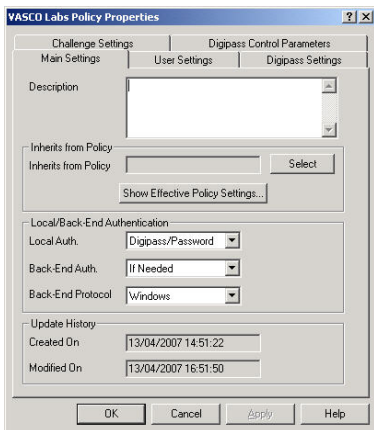


Figure 13: VM configuration (3)

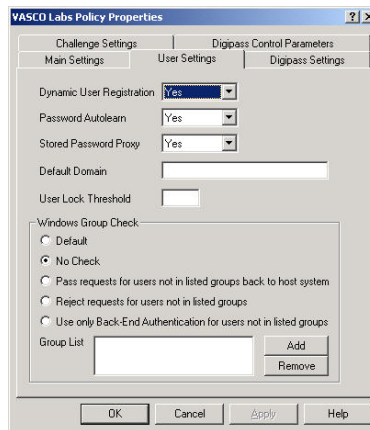


Figure 14: VM configuration (4)

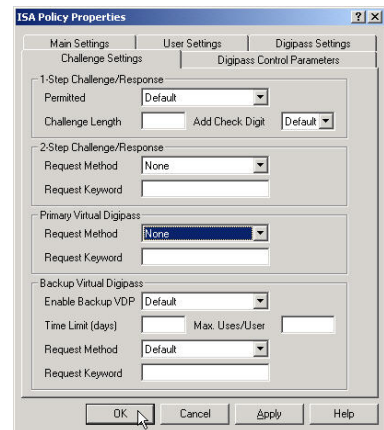


Figure 15: VM configuration (5)

6.2 Component configuration

For testing purposes you can change the existing RADIUS Client (default RADIUS client that listens for all connections) by right-clicking and choose **Properties**.

If you already use the default RADIUS client, it would be better to create a new RADIUS component.

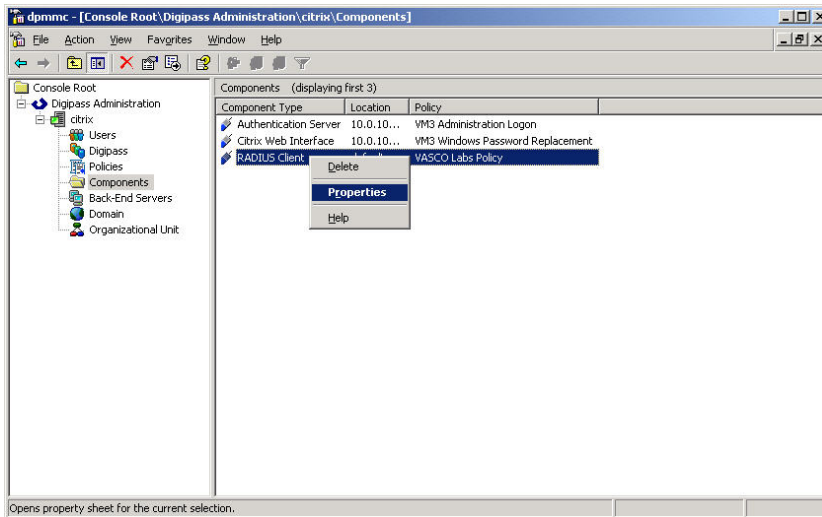


Figure 16: VM configuration (6)

In the policy field you should find your **newly created policy**. Fill in the **shared secret** you entered also in the RADIUS server properties on the ISA server. Click **Create**.

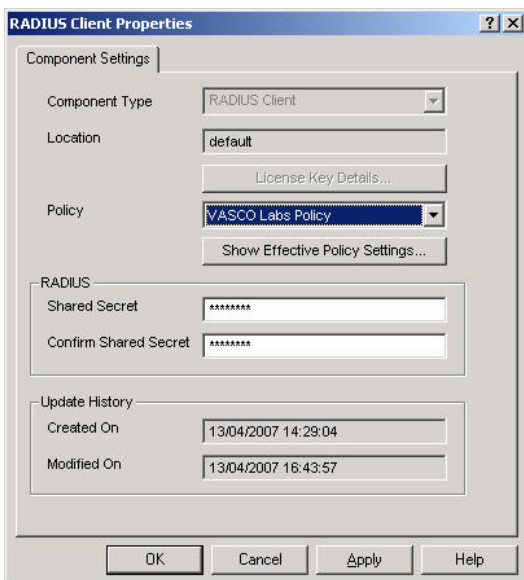


Figure 17: VM configuration (7)

All configuration is done by now. The next chapter shows you how to add a user manually. In our policy we enabled the Dynamic User Recognition (DUR). So users who get verified through the Active Directory, and are not known in the local database, are automatically added. It also shows how to assign a DIGIPASS to a user.

7 User configuration

The **user creation** steps you will find in this chapter are optional when you didn't activate the option **Dynamic User Registration (DUR) and/or Password Autolearn** in your policy settings.

The assignment of a DIGIPASS can happen manually as explained in the steps below. The user creation and DIGIPASS assignment steps depend on which database back-end you installed VACMAN Middleware. Either you installed it with an ODBC back-end or with an Active Directory back-end.

7.1 ODBC installation

7.1.1 User creation

User creation, while using an ODBC back-end, will happen in the DIGIPASS Administration MMC. Right-click the Users folder and select **New User ...**.

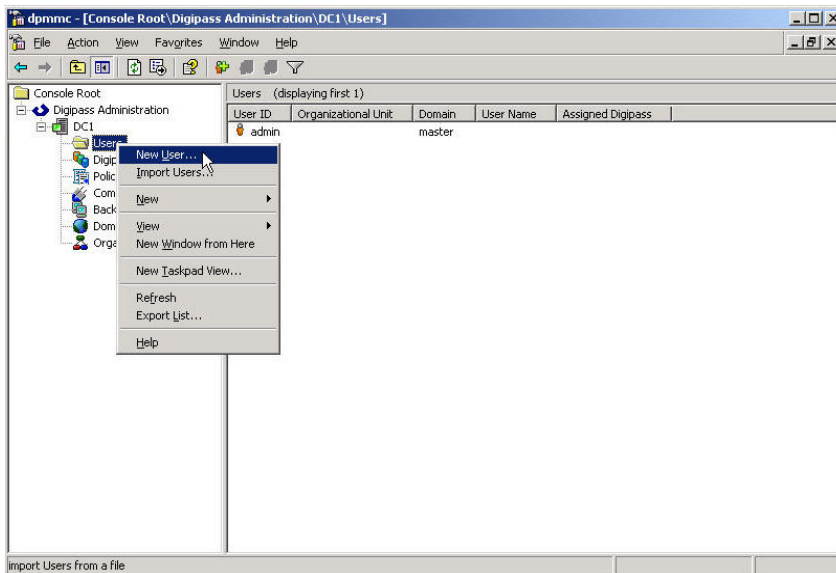


Figure 18: ODBC User Creation (1)

Fill in the username and password fields. Optionally choose the right domain and Organizational Unit and click the **Create** button.

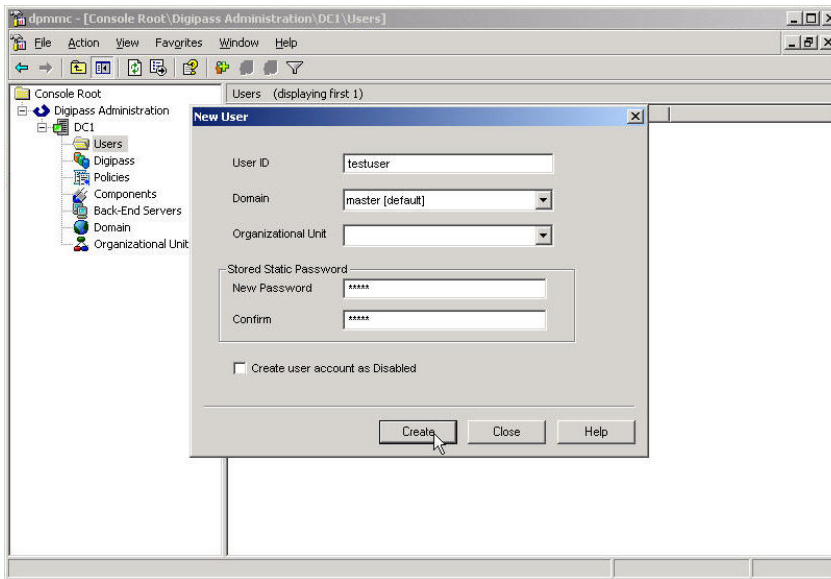


Figure 19: ODBC User Creation (2)

The user will now show up in the Users list of you DIGIPASS Administration MMC. At this point it will be exactly the same as when Dynamic User Recognition (DUR) was enabled.

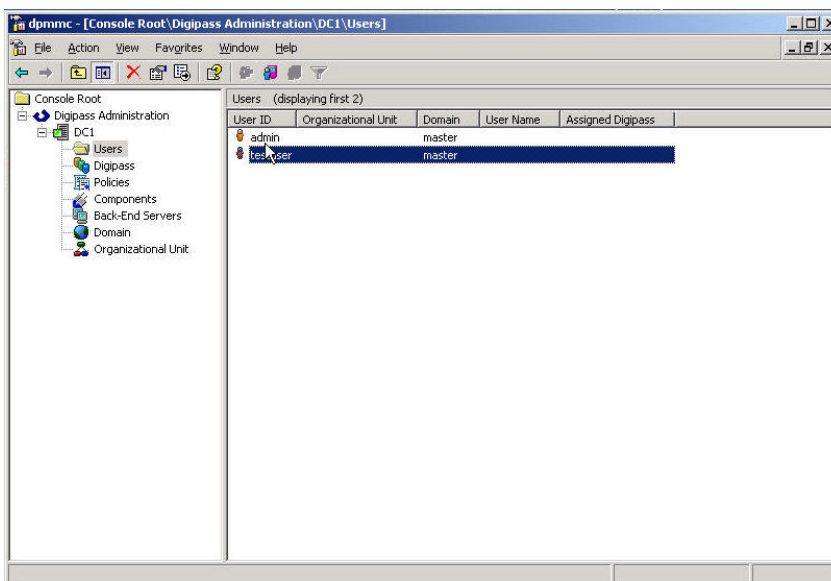


Figure 20: ODBC User Creation (3)

7.1.2 Import DIGIPASS

Right-click the DIGIPASS folder and select **Import DIGIPASS...**

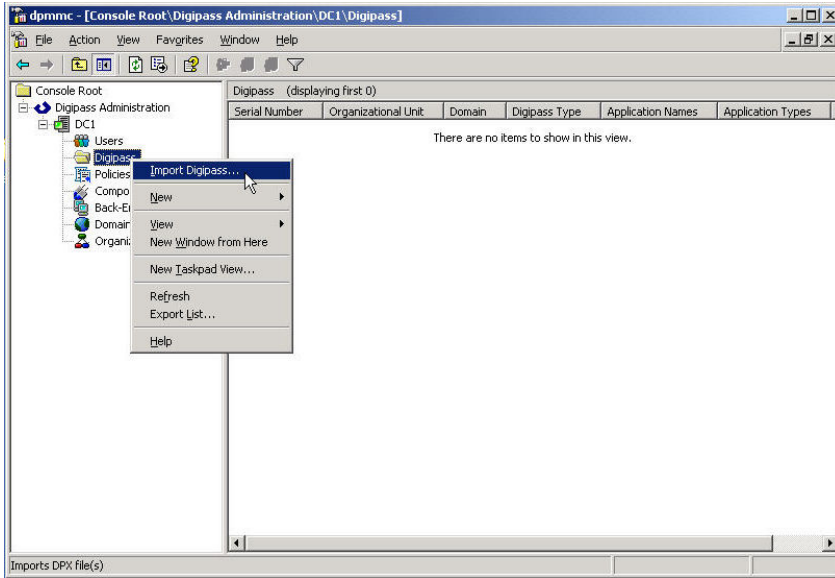


Figure 21: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import ...** buttons above and below the Show Applications button.

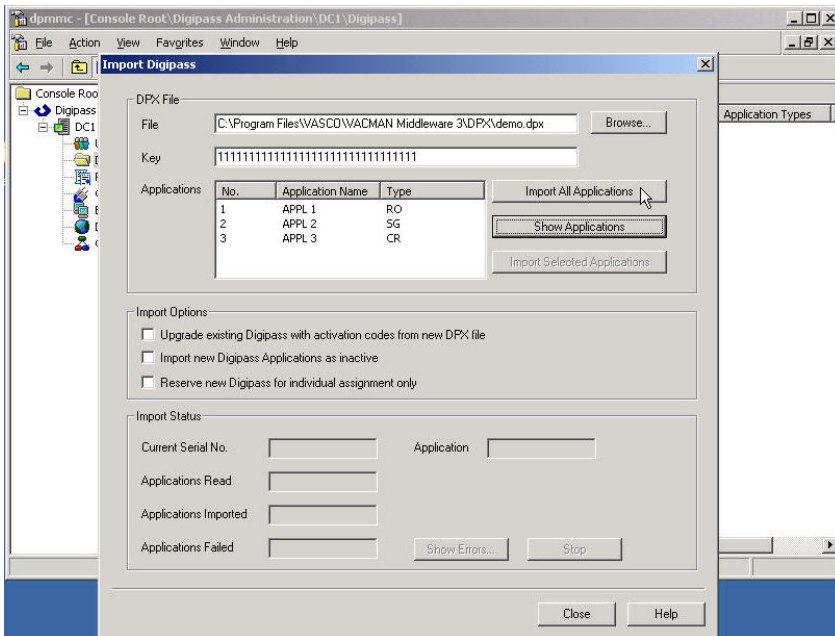


Figure 22: Import DIGIPASS (2)

When the DIGIPASS is imported successfully you will receive a confirmation message.

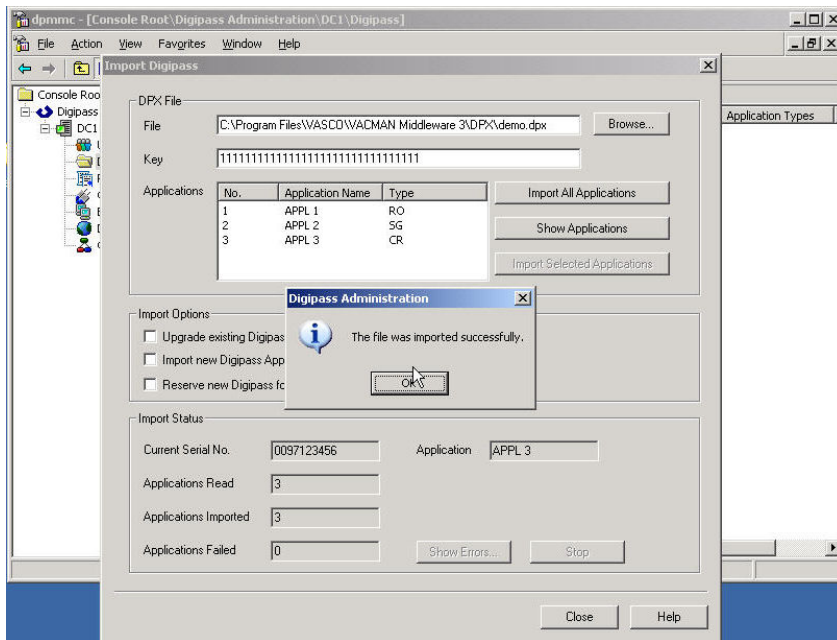


Figure 23: Import DIGIPASS (3)

7.1.3 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.

Right-click a user and select **Assign DIGIPASS...** or ...

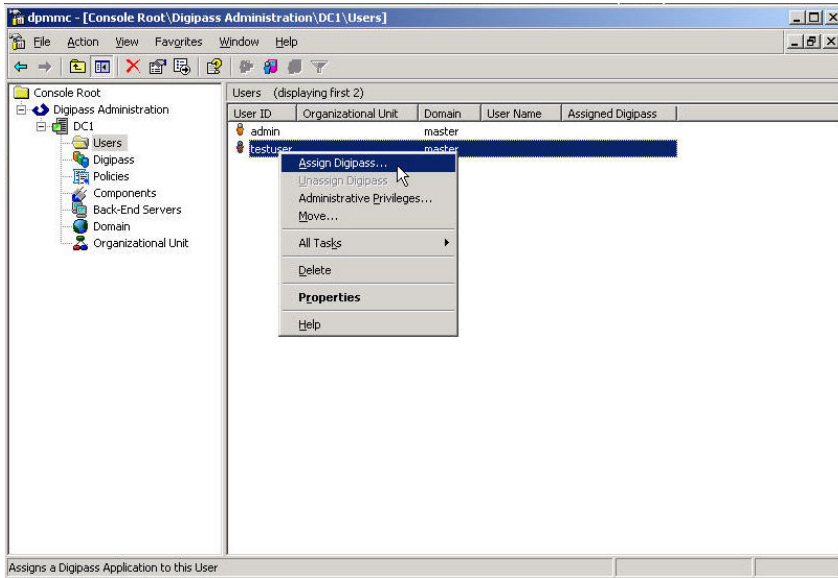


Figure 24: DIGIPASS assignment (1)

... you can right-click a DIGIPASS and select **Assign ...**

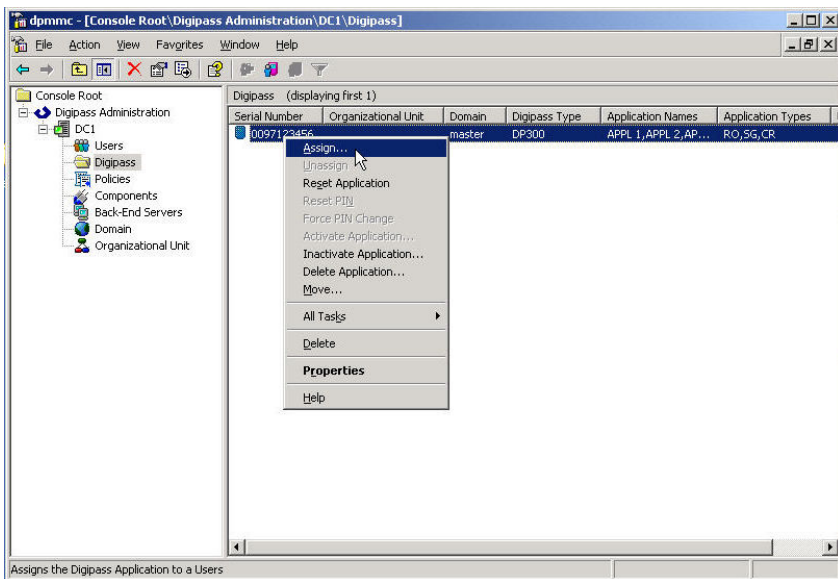


Figure 25: DIGIPASS assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

Notice: If no users show up, make sure the domains of the DIGIPASS and the user match.

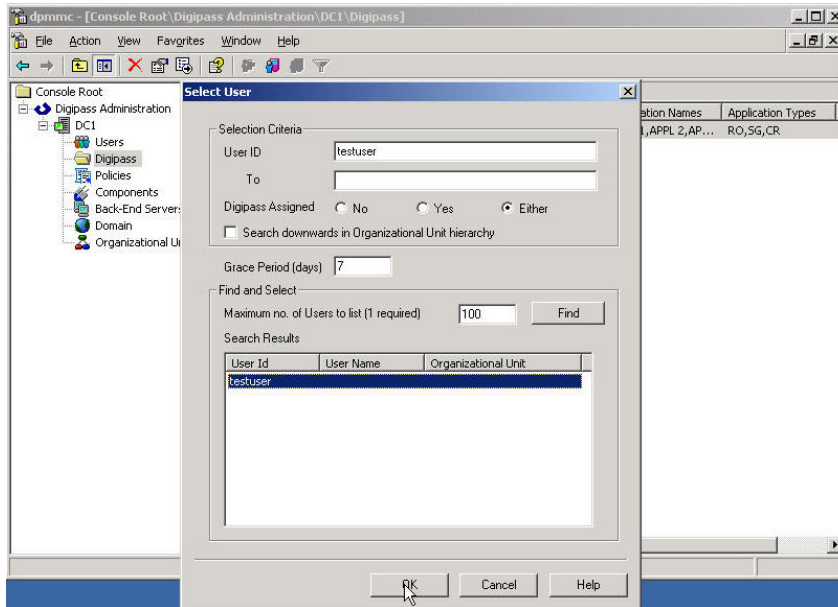


Figure 26: DIGIPASS assignment (3)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or search through serial number. Leaving all options blank will show all possibilities in the same domain.

When the DIGIPASS gets successfully added to your user you will get a confirmation message.

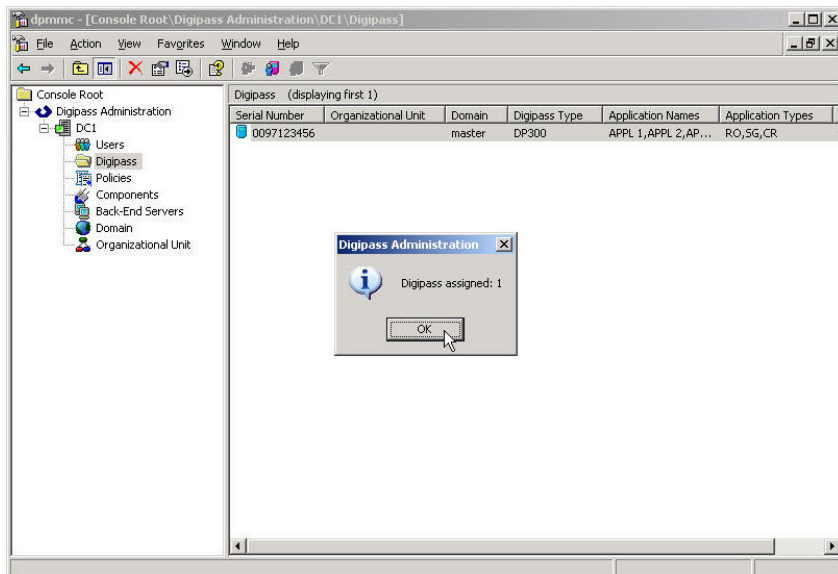


Figure 27: DIGIPASS assignment (4)

7.2 Active Directory installation

7.2.1 User creation

User creation, while using an Active Directory back-end, will happen in the **Active Directory Users and Computers MMC**. Right-click a user and select **Properties**. This can happen automatically when the Dynamic User Registration (DUR) option in the policy settings is active.

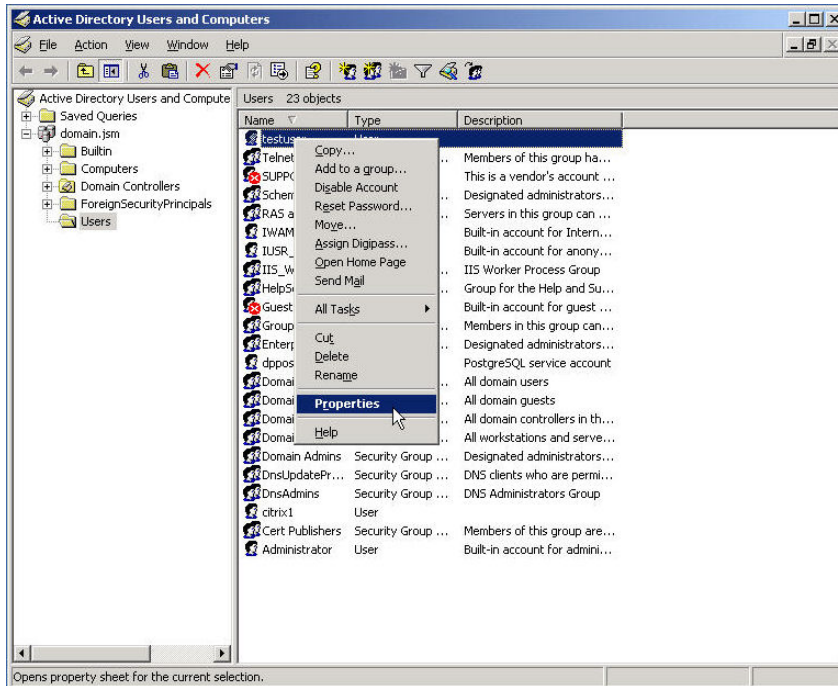


Figure 28: Active Directory User Creation (1)

In the **DIGIPASS User Account** tab you will see a field to manually add a password. This can also be automatically filled by enabling the Password Autolearn option in the policy settings.

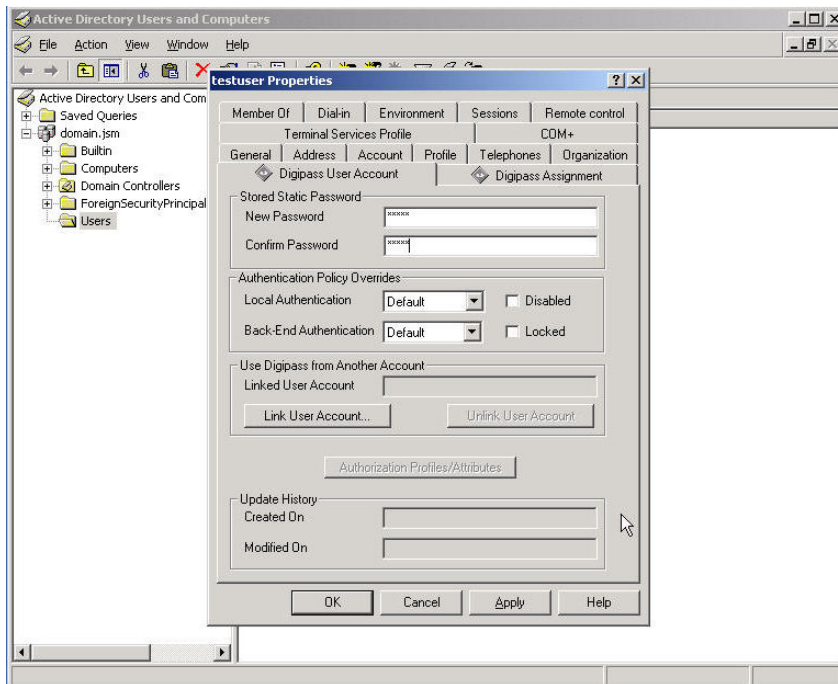


Figure 29: Active Directory User Creation (2)

After clicking the Apply button you will see the Update History fields being filled with the current date and time. When these fields are filled it means the DIGIPASS account exists and can be used.

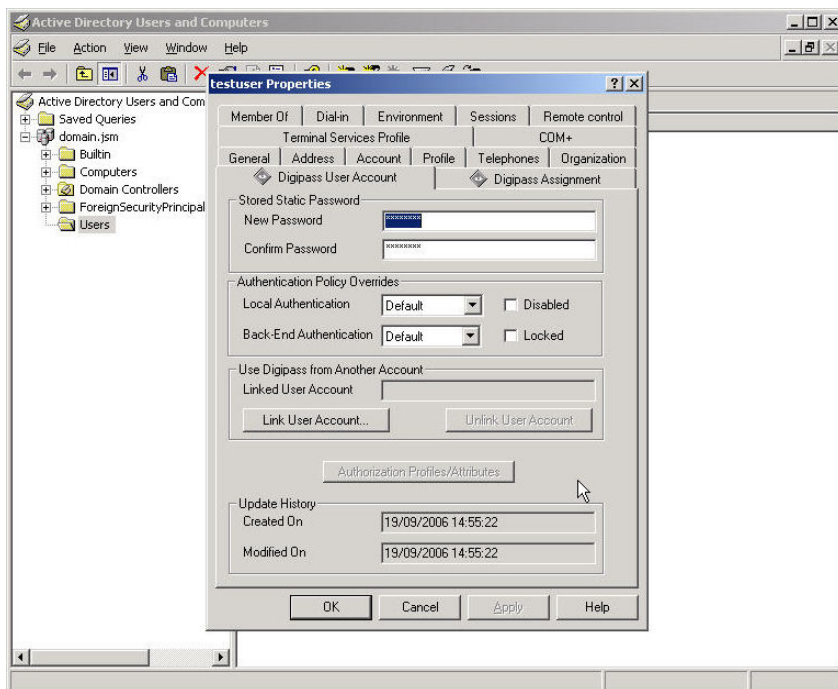


Figure 30: Active Directory User Creation (3)

7.2.2 Import DIGIPASS

To make sure you can see the DIGIPASS folders in the MMC, go to **View** and select the **Advanced Features**. This way you will see the DIGIPASS folders.

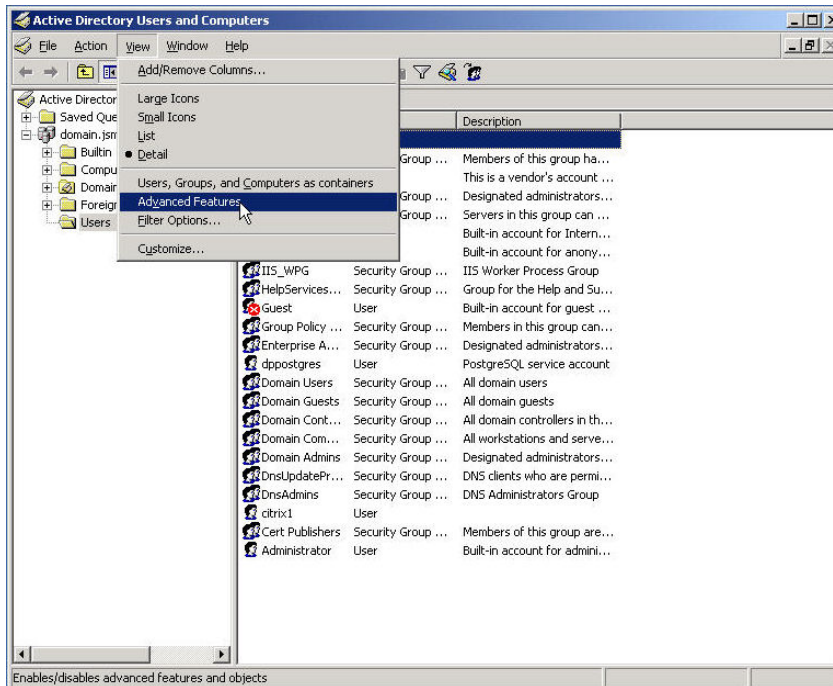


Figure 31: Import DIGIPASS (1)

Right-click the **DIGIPASS-Pool** folder and select **Import DIGIPASS ...**

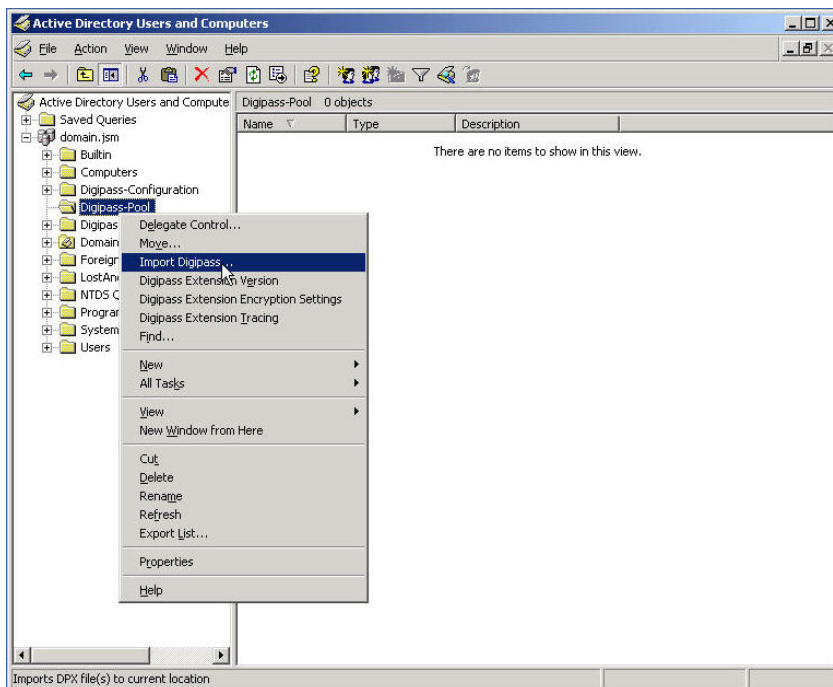


Figure 32: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import ...** buttons above and below the Show Applications button.

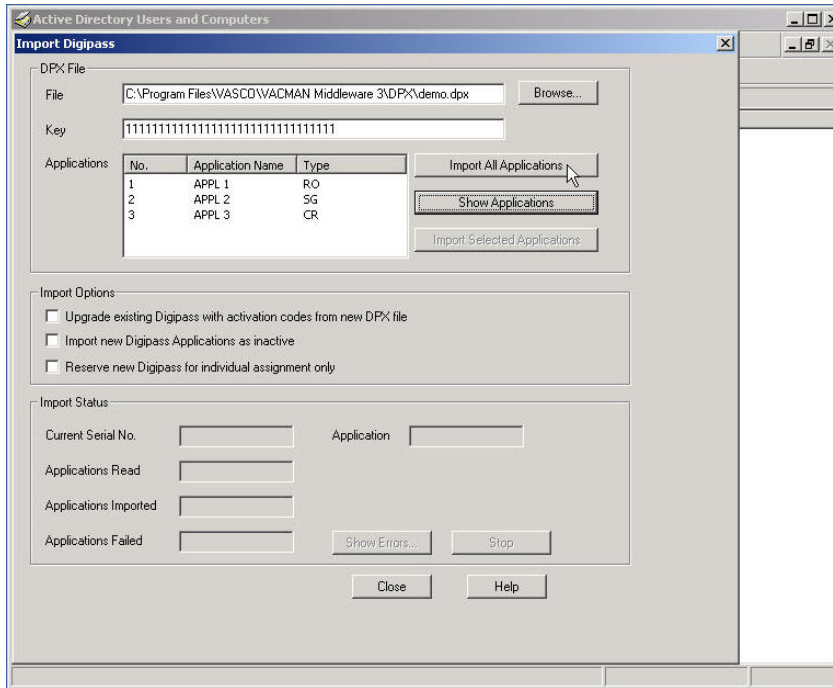


Figure 33: Import DIGIPASS (1)

When the DIGIPASS is imported successfully you will receive a confirmation message.

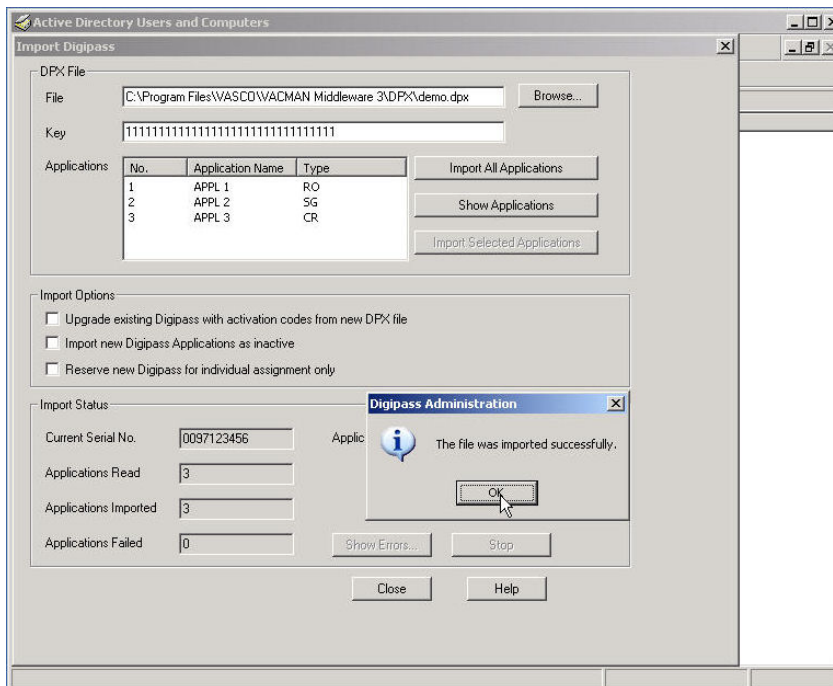


Figure 34: Import DIGIPASS (1)

7.2.3 DIGIPASS assignment

There are two possible ways to assign a user to a DIGIPASS. 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.

Right-click a **User** and select **Assign DIGIPASS...** or ...

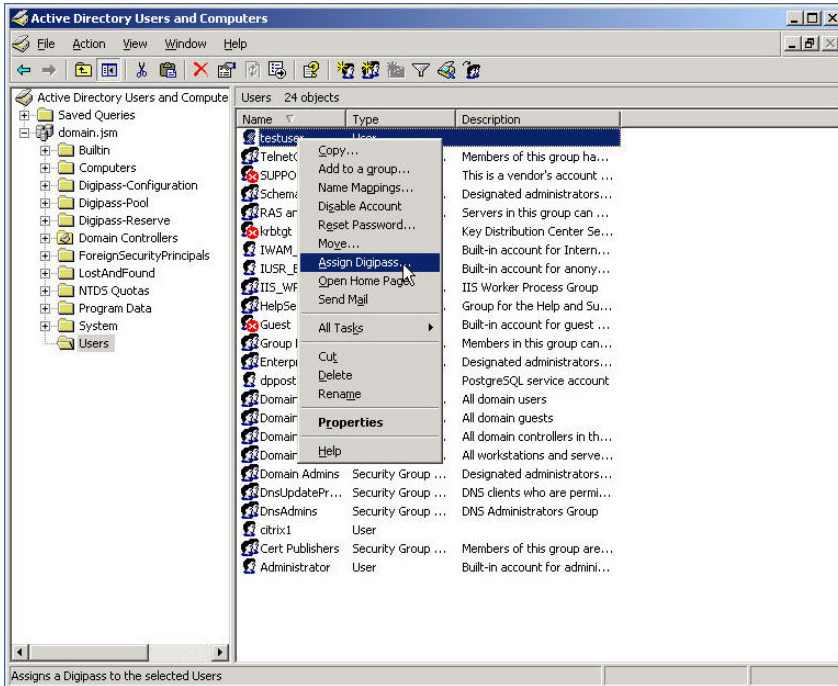


Figure 35: DIGIPASS Assignment (1)

... right-click a **DIGIPASS** and select **Assign DIGIPASS ...**

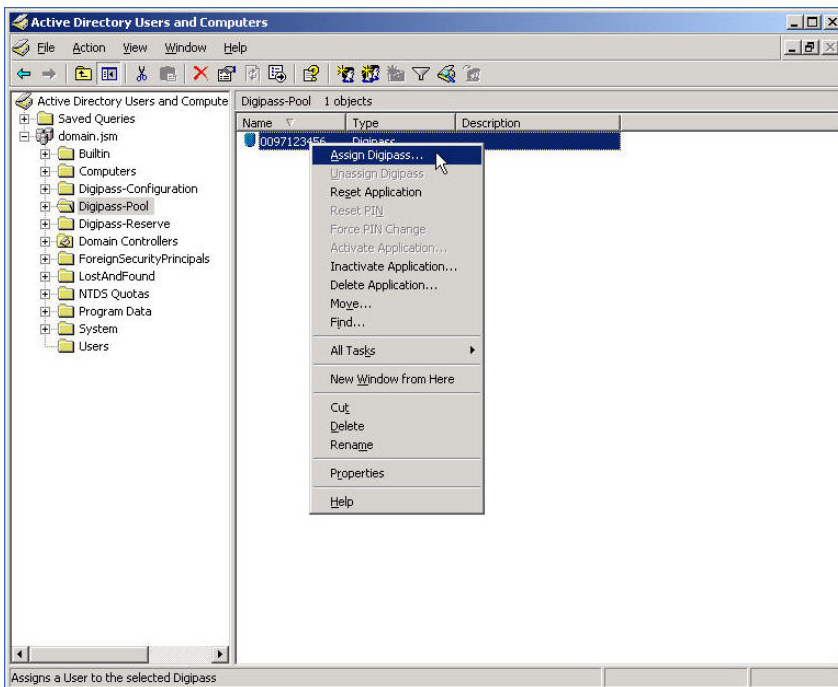


Figure 36: DIGIPASS Assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

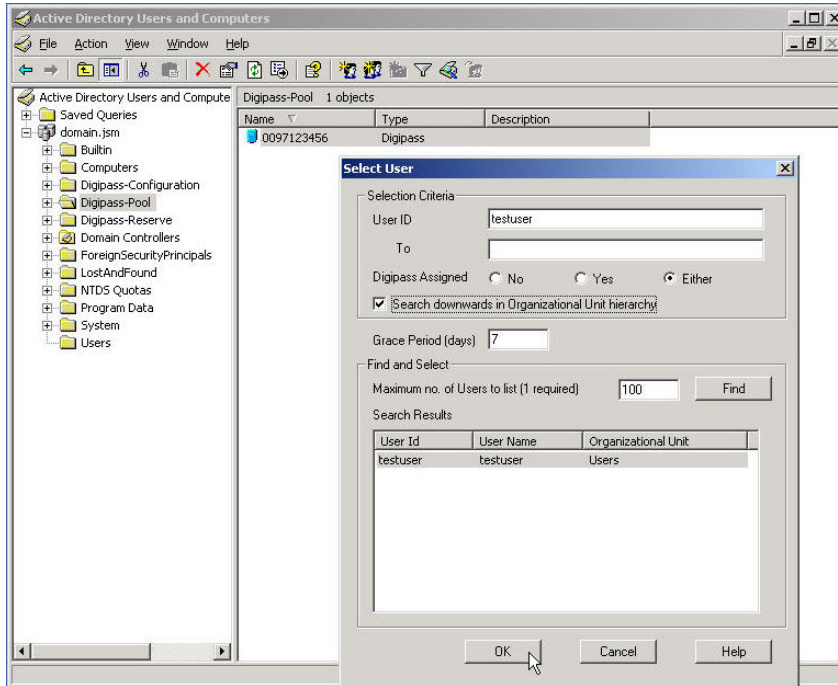


Figure 37: DIGIPASS Assignment (4)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or through serial number. Leaving all options blank will show you all possibilities. Remember to check the **“Search upwards ...”** checkbox.

8 GajShield VPN test

Open the VPN Client, select the correct tunnel and click the **Open Tunnel** button.

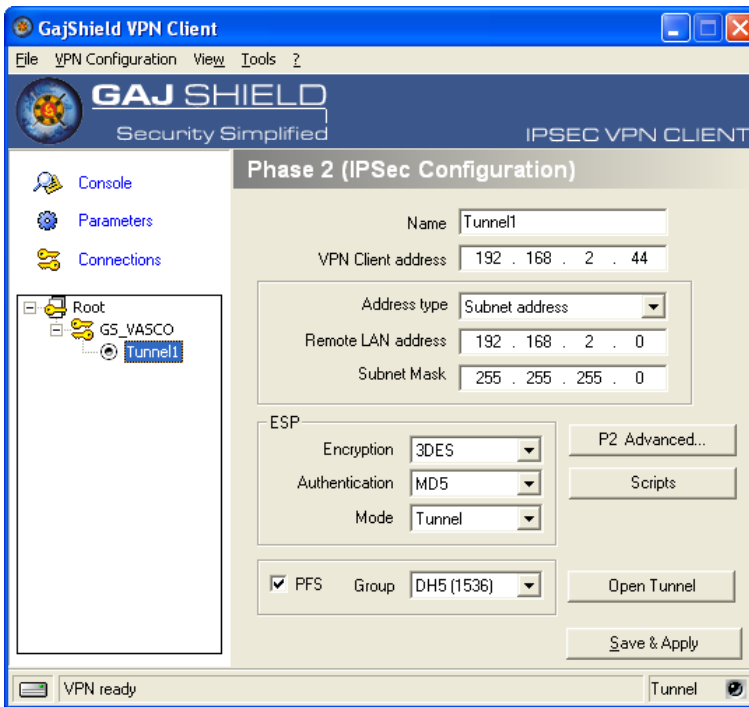


Figure 38

Enter the **Login** and a **One-Time Password** in the fields and click **OK**.

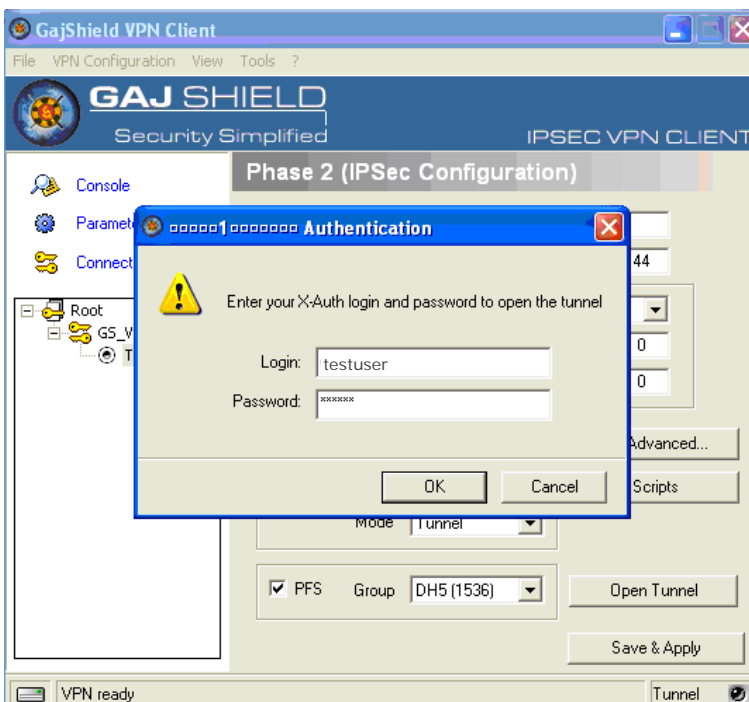


Figure 39

The VPN Tunnel will be opened and the client will be connected to the server.

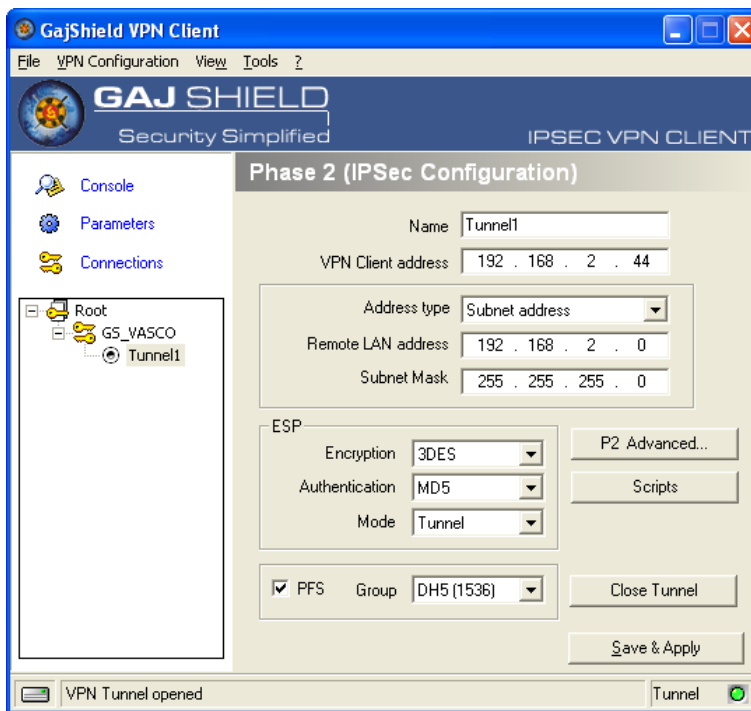


Figure 40

9 VACMAN Middleware features

9.1 Installation

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

9.1.1 Support for Windows 2000, 2003, IIS5 and IIS6

VM can be installed on Windows 2000 and Windows 2003. Web modules exist for IIS5 and 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).

9.1.2 Support for ODBC databases and Active Directory

Any ODBC compliant database can be used instead of the default PostgreSQL database (MS SQL Server, Oracle). Since Version 2.3 of VACMAN Middleware, AD is **not only** intended for storage of DIGIPASS anymore, but configuration and management of your DIGIPASS infrastructure is now also full integrated into the AD management tools. This option requires an AD schema update.

9.2 Deployment

Several VACMAN Middleware features exist to facilitate deployment. Combining these features provides different deployment scenarios from manual to fully automatic.

9.2.1 Dynamic User Registration (DUR)

This feature allows VM 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 VM database.

9.2.2 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 VM database, VM can verify it with the back-end RADIUS server or the Windows domain controller and, if correct, store it for future use.

9.2.3 Stored Password Proxy

Allows VM 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.

9.2.4 Authentication Methods

Different authentication methods can be set on server level and on user level: local authentication (VM 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).

9.2.5 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.

9.2.6 DIGIPASS Self Assign

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

9.2.7 DIGIPASS Auto Assign

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

9.2.8 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.

9.2.9 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 VACMAN Middleware 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 VACMAN Middleware, 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.

9.3 Administration

9.3.1 Active Directory Users and Computers Extensions

Since VACMAN Middleware version 2.3, Managing the users and DIGIPASS can be done within the Active Directory Users and Computers section. Selecting the properties of a user, offers complete User-DIGIPASS management.

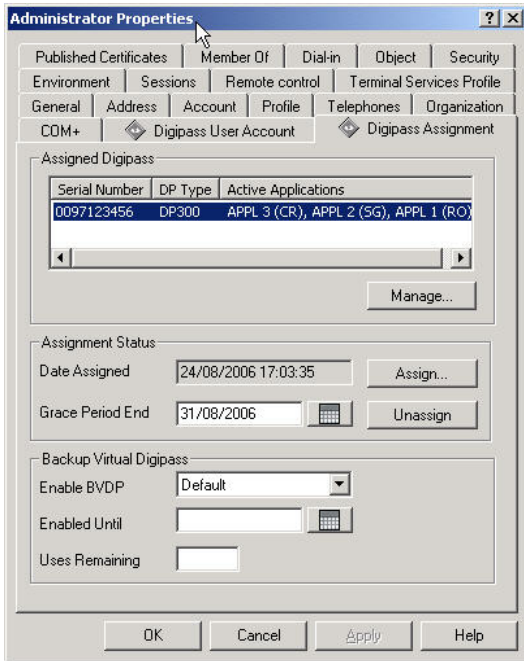


Figure 41: VM Features (1)

9.3.2 Administration MMC Interface

A highly intuitive Microsoft Management Console (MMC) exists to administer the product. An Audit Console is available to give an instant view on all actions being performed on the VM. Both can be installed on the VM server itself or on a separate PC.

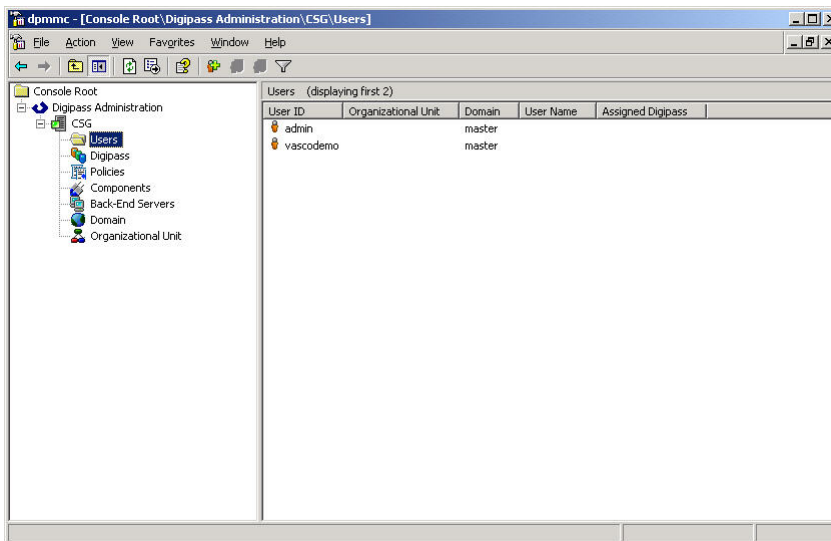


Figure 42: VM Features (2)

9.3.3 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 VM database, to do a change PIN (Go-1/Go-3 DIGIPASS), to do a DIGIPASS test.



Figure 43: VM Features (3)

9.3.4 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.

9.3.5 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. A user can be created that only has the rights to unlock a DIGIPASS.

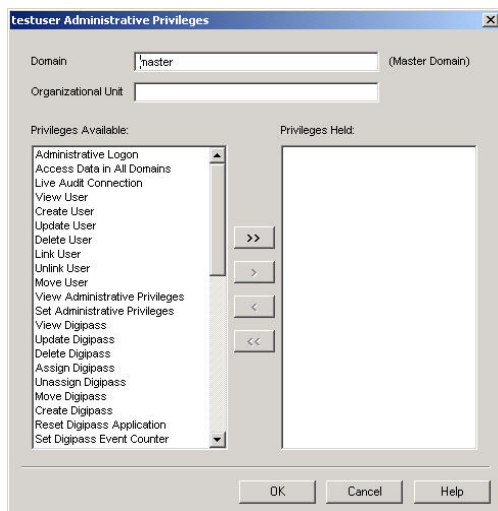


Figure 44: VM Features (4)

10 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.