

DIGIPASS Authentication for **GajShield GS Series**

With Vasco VACMAN Middleware 3.0





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

D	IGI P/	ASS /	Authentication for GajShield GS Series1
Di	isclai	mer	2
Та	able o	of Co	ntents3
1	Ove	ervie	w5
2	Pro	blen	n Description5
3	Sol	utior	า5
	3.1	VPN	I Client5
4	Тес	hnic	al Concept
	4.1	Gen	eral overview
	4.2	Gaj	Shield prerequisites6
	4.3	VAC	CMAN Middleware Prerequisites
5	Gaj	Shie	Id configuration7
	5.1	RAD	0IUS Server
	5.2	RAD	DIUS Users
	5.3	VPN	I Settings 12
	5.4	Fire	wall Settings 13
6	VA	CMAI	N Middleware14
	6.1	Poli	cy configuration
	6.2	Con	nponent configuration16
7	Use	er co	nfiguration
	7.1	ODE	3C installation 17
	7.1	. 1	User creation
	7.1	.2	Import DIGIPASS
	7.1	.3	DIGIPASS Assignment
	7.2	Acti	ve Directory installation
	7.2	. 1	User creation



	7.2.2	Import DIGIPASS	25
	7.2.3	DIGIPASS assignment	27
8	GajShie	eld VPN test2	9
9	VACMA	N Middleware features3	1
	9.1 Inst	tallation	1
	9.1.1	Support for Windows 2000, 2003, IIS5 and IIS6	1
	9.1.2	Support for ODBC databases and Active Directory	?7
	9.2 Dep	oloyment	1
	9.2.1	Dynamic User Registration (DUR)	?7
	9.2.2	Autolearn Passwords	1
	9.2.3	Stored Password Proxy	1
	9.2.4	Authentication Methods 3	?1
	9.2.5	Policies	2
	9.2.6	DIGIPASS Self Assign	2
	9.2.7	DIGIPASS Auto Assign	2
	9.2.8	Grace Period	2
	9.2.9	Virtual DIGIPASS	2
	9.3 Adr	ninistration	3
	9.3.1	Active Directory Users and Computers Extensions	3
	9.3.2	Administration MMC Interface	3
	9.3.3	User Self Management Web Site	24
	9.3.4	Delegated administration	?4
	9.3.5	Granular access rights	?4
10) About	VASCO Data Security	5

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.

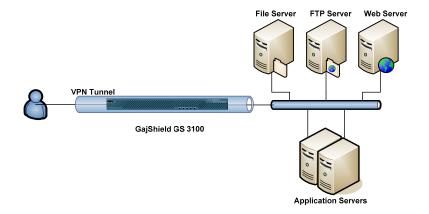


Figure 1: VPN Client



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 4005
- 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: <u>https://192.168.2.180</u>.

GajShield: Web based Administration and Management Tool - Windows Internet Explorer	provided by Vasco Data Security		@_X
C . R Mps://192.168.2.180/admin/		💌 😵 Gertificate Error 🤧 🛪 Google	P -
Ele Edit Yerr Favorites Icols Help			e . •
👙 🤣 🏉 GajShield: Web based Administration and Managemen			
GajShield SecureGate v5			502
Eirewall Management		Firewall Management	
	GajShield Firewall Management		
	Username superuser		
	Password		
	Login		
	Copyright © GajShield Inforach (I) Firt. Ltd. All rights reserved		
		😱 😝 Internet	₹100% •

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.

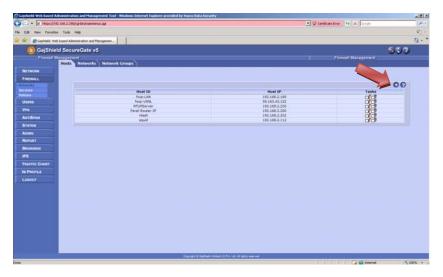


Figure 3: RADIUS Server (1)

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

• R https://192.168.2.180/cgi-bin/mainmenus.gg	💌 😧 Centificate Error 🧤 🗶 Google	
Edit View Figurantes Ecols Help		
Gaishield: Web based Administration and Managemen		- 0
6 GajShield SecureGate v5	S.0	
Firewall Management	Firewall Management	
Hosts Networks Network Groups		
IETWORK		
REWALL		
works		0
vices	Configure Hosts	
Host Id	vasco-server	
Host IP	192.168.2.50 Add	
NTISPAM	Add	
VIGTAM		
DMIN		
IEPORT		
Rowsing		
25		
RAFFIC CHART		
RAFFIC CHART		
PROFILE	Copyrget & Späthant solvana (). Pro 11: 21: 24 open annora	

Figure 4: RADIUS Server (2)

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



 Mtps://192.168.2.180/cpi 	i-bin/mainmenus-ggi	💌 🤡 Certif	Kate Error 🌴 🗙 Google	-10
Edit Yen Favorites Jooks Hel				¢.
 Edit Vew Favorites Tools Hell Gatshield: Web based Administration 				- 0
(GajShield Secure			500	
Firewall Management			Firewall Management	
Hosts	Networks Network Groups			
NETWORK				
FIREWALL				
Retworks			00	
Sentces	Host ID	Host IP	Tasks	
	fwip-LAN	192.168.2.180		
Users	fwip-VSNL NTUMServer	59.163.43.152 192.168.2.220		
VPN	Panel-Router-IP	192.168.2.20		
and the second se	ritesh	192.168.2.200	13	
ANTISPAM	squid	192.168.2.112	11	
SYSTEM	vasco-server	192.168.2.50	11	
REPORT BROWSING				
BROWSING IPS TRAFFIC CHART				
BROWSING				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE				
BROWSING IPS TRAFFIC CHART IM PROFILE	County & School	unhan ij Po 10 Argin werd		

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 **Delta** button on the right side of the screen to add RADIUS users.

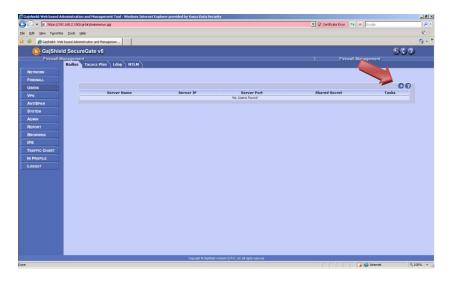


Figure 6: RADIUS Users (1)

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.

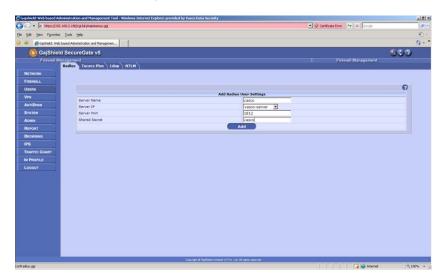


Figure 7: RADIUS Users (2)



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".

ie Edit View Favorites	Icols Help		
Back • 🕥 • 🗙	🗟 🏠 🔎 Search 🤺 Favorites 🕢 🔗 🍓 🔳 - 📒	8	
dress 🕘 https://192.168.2.18			💌 🛃 Go 🛛 Li
~	SecureGate v5		502
Firewall Man			000
	olicy Tunnels Local IPsec Key Reserved IPs Advance	d Setup Restart VPN	
NETWORK			
FIREWALL			
Users			0
VPN	Advanced IPSE		
IPsec	Unique Ids Override Default MTU value:	⊙ Yes ◯ No	
Certificates	NAT Traversal	1420	
PPTP	Strict CRL Policy	O Yes ⊙ No	
Local User	Mod		
ANTISPAM			
SYSTEM	Authentication Type	radius V	
ADMIN	Authentication Type		
REPORT			
BROWSING			
IPS			
TRAFFIC CHART			
IM PROFILE			
LOGOUT			
	Copyright @ GajShield Infotech (i) Pvt. Ltd. All		

Figure 9: VPN Settings



Firewall Settings 5.4

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.

dress 🗃 https://192.168.2.	180/coi-bin/mair												🗸 🄁 Go	Links
() GajShield													50	
Firewall Ma		bate 1	~•										- 30	0
Priewanina	Quick Setu	Ru	les Bandw	idth 🔪 Insta	II Policies	Backu	p Rul	es A	lmin Ips					
NETWORK	•	to LAN	Both-Branch	GajAccess	TWID-LAN	accept	yes	active	derault	On	no	none		
FIREWALL	7	Any to VSNL	fwnet-LAN	ping	any	accept	yes	active	test	Always On	no	none	ddo,	
Services Policies	0	LAN to LAN	Both-Branch	squid	fwip-LAN	accept	yes	active	default	Always On	no	none	d đo	
Users	9	VSNL to VSNL	fwip-VSNL	http https	internet	accept	yes	active	default	Always On	no	none	ddo	
VPN ANTISPAM	10	to LAN	fwip-LAN	NTLM	NTLMServer	accept	yes	active	default	Always On	no	none	dø.	
System	11	to LAN	GajShield- MBP	ping	fwip-LAN	accept	yes	active	default	Always On	no	none	d đe	
ADMIN	12	to LAN	fwip-LAN	Idaptop	fwnet-LAN	accept	yes	active	default	Always On	no	none	ddo	
BROWSING	13	to LAN	fwip-LAN	Idapudp	fwnet-LAN	accept	yes	active	default	Always On	no	none	d d'o>	
IPS TRAFFIC CHART	14	LAN to LAN	fwip-LAN	ssh	Both- Branch	accept	yes	active	default	Always On	no	none	dđo	
IM PROFILE	15	LAN to LAN	fwip-LAN	vasco	vasco- server	accept	yes	active	default	Always On	no	none	ddo	
Logout	16	VSNL to VSNL	any	IPSec-VPN	fwip-VSNL	accept	yes	active	default	Always On	no	none	d d'a•	
	17	Any to LAN	fwnet-LAN	ping	fwnet-LAN	accept	yes	active	default	Always On	no	none	d đo	

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**.

🚡 dpmmc - [Console Root\Digipass	Administration\ISA2006]		-OX
📸 Eile Action Yiew Favorites y	<u> V</u> indow <u>H</u> elp		_ & ×
← → 🗈 💽 🗙 🔂 😫			
Console Root	ISA2006		
Digipass Administration	Name		
ISA2006	the Users		
Digipass	Contraction Contra		
Polid New Policy	onents		
Com A	End Servers		
Dorr	in		
Org. New Window from	h Here hizational Unit		
Help			
creates a 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.

Name	VASCO Labs Policy.	
Description		<u>_</u>
		-
🖸 Inherit default	t settings from another policy	
Inherit from		_
	ngs from another Policy	<u> </u>
	ngs from another Policy	

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

Main Settings tab • o Local auth .: Digipass/Password If Needed o Back-End Auth.: • 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 o 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.

ASCO Labs Policy Properties	<u>?</u> ×	VASCO Labs Policy Properties	? 🗙 ISA Polic	y Properties	?)
	igipass Control Parameters	Challenge Settings Digipass Control Main Settings User Settings Dir		ain Settings User Settings Challenge Settings Dining	Digipass Settings
Main Settings User Settings	Digipass Settings	Main Settings User Settings Dig	poor counge		ass Control Parameters
Description	×	Dynamic User Registration Yes		p Challenge/Response nitted Default	•
	*	Password Autolearn Yes	Cha	illenge Length Add Check	Digit Default 💌
Inherits from Policy		Stored Password Proxy Yes	-2-Ste	p Challenge/Response	
Inherits from Policy	Select	Default Domain	Reg	quest Method None	×
Show Effective Policy	Settings	User Lock Threshold	Req	quest Keyword	
Local/Back-End Authentication		- Windows Group Check	Prima	ary Virtual Digipass	
Local Auth. Digipass/Password	•	C Default	Req	uest Method None	<u> </u>
Back-End Auth, If Needed	•	No Check	Req	quest Keyword	
1		C Pass requests for users not in listed groups back to h	nost system Back	up Virtual Digipass	
Back-End Protocol Windows	·	C Reject requests for users not in listed groups	Ena	ble Backup VDP Default	•
- Update History		C Use only Back-End Authentication for users not in lis	ted groups Time	e Limit (days) Max. Uses	/User
Created On 13/04/2007 14:51:2	22	Group List	Add Beg	uest Method Default	•
Modified On 13/04/2007 16:51:5	50	F	Remove	auest Keyword	_
•				new volument	
OK Cancel	Apply Help	OK Cancel Apply	Help	OK Cancel	Apply Help
	Colory Holp	Cancer Eppy			

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.

🚡 dpmmc - [Console Root\Digipass	Administration\citrix\Co	mponents]		_ 🗆 🗵
📸 Eile Action View Favorites 🛛	/indow <u>H</u> elp				_8×
← → 🗈 🖪 🗙 😭 😫	0 0 0 T				
Console Root	Components (displaying f	irst 3)			
Digpass Administration dritx drit	Authentication Server Authentication Server Crinx Web Interface TADUS Client Ped Ped Hels	10.0.10 te	Policy VM3 Administration Logon VM3 Windows Password Replacement VASCO Labs Policy		
Opens property sheet for the current selec	tion.			ļ	

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**.

	· · · · · · · · · · · · · · · · · · ·					
Component Type	RADIUS Client					
Location	default					
	License Key Details					
Policy	VASCO Labs Policy					
	Show Effective Policy Settings					
RADIUS		Ť.				
Shared Secret	*****					
Confirm Shared Secret	*****					
Update History		-				
Created On	13/04/2007 14:29:04					
Modified On	13/04/2007 16:43:57					

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.



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 backend 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**

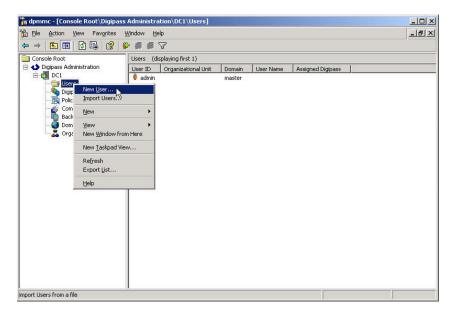


Figure 18: ODBC User Creation (1)



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

🚡 dpmmc - [Console Root\Digipa	ss Administration\DC	1\Users]		_OX
🚡 Elle Action View Favorites	<u>W</u> indow <u>H</u> elp			_ 5 ×
← → 🗈 🖬 🔂 😼 😫	🍄 🖪 🖉 🍸			
Console Root	Users (displaying f	irst 1)		
🗄 📣 Digipass Administration	w User		×	
DC1				
- Cigipass	User ID	testuser		
Components Back-End Servers	Domain	master [default]	•	
Organizational Unit	Organizational Unit		-	
	Stored Static Passwo			
	New Password	*****		
	Confirm	*****		
	Create user acc	a set a set de la constante de		
	j Create user acci	ount as bisabled		
		Create Clo	Help	

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.

dpmmc - [Console Root\Digipas	s Administration\DC1\U	ers]			
Elle Action View Favorites	Window Help				_18 ×
> → 🗈 📧 🗙 🗗 🖳 🖆	9 9 9 1 7				
Console Root	Users (displaying first 2)			
🗄 📣 Digipass Administration	User ID Organizatio	nal Unit Domain	User Name	Assigned Digipass	
🖻 📶 DC1	🕴 admin	master			
- 🔄 Users - 隆 Digipass	🔮 tes ser	master			
Policies					
Components					
- 🗓 Back-End Servers					
Domain					
- 🌄 Organizational Unit					





7.1.2 Import DIGIPASS

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

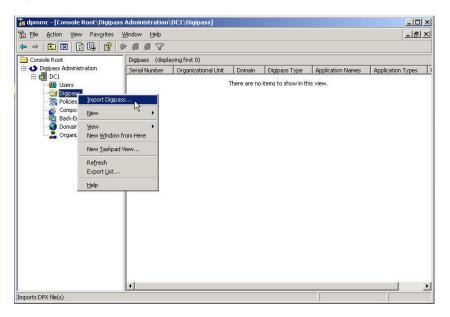


Figure 21: Import DIGIPASS (1)

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.

宿 dpmmc - [Consc	ole Root\Digipass Administration\DC1\Digipass]	
🚡 Eile Action y	iew Favgrites <u>Wi</u> ndow <u>H</u> elp	X
	port Digipass	×
Console Roo	r DPX File	
🖻 📣 Digipass	File C:\Program Files\VASCO\VACMAN Middleware 3\DPX\demo.dpx Browse	Application Types
- 📅 τ	Kev 111111111111111111111111	
	Applications No. Application Name Type Import All Applications	
∰ I ∰ I ∰ I ∰ I ∰ I	2 APPL 2 5G Show Applications	
⊢ <u>&</u> (3 APPL 3 CR	
	Import Selected Applications	
	r Import Options	
	Upgrade existing Digipass with activation codes from new DPX file	
	Import new Digipass Applications as inactive	
	Reserve new Digipass for individual assignment only	
	└ Import Status	
	Current Serial No. Application	
	Applications Read	
	Applications Imported	
	Applications Failed Show Errors Stop	
·	Applications Failed Show Errors Stop	
-		
	Close Hel	p

Figure 22: Import DIGIPASS (2)



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

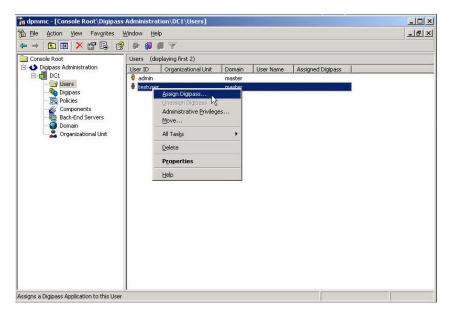
È Eile Action ⇔ → ΓετΩΩ	<u>Vi</u> ew Fav <u>o</u> rites Import Digipass	Window	Help	and the second		
Console Roo						
Digipass	DPX File					Application Types
🖻 🧖 DC1	File	C:\Progr	am Files\VASCO\VACM	1AN Middleware 3\E	PX\demo.dpx Browse	()pp/cscion ()poo
	Key	1111111	111111111111111111111	1111111		
			1	1	T I	
É :	Applications	No.	Application Name APPL 1	Type RO	Import All Applications	
		2	APPL 2 APPL 3	SG	Show Applications	
		3	AFFLJ	CK	1	
	- Import Options		Digipass Admin	istration	Import Selected Applications	
	Import Options Upgrade e Import nev	existing Dig v Digipass	ipas 🗼 The f	iistration ile was imported suc		
	Upgrade e	existing Dig v Digipass	ipas 🗼 The f	ile was imported su		
	Upgrade e Import nev	existing Dig v Digipass new Digipa	ipas 🗼 The f	ile was imported su		
	Upgrade e Import nev Reserve n Import Status Current Serial	existing Dig v Digipass new Digipa No.	ipas ipas The f App ss fc [ile was imported suc	cessfully.	
	Upgrade e Import new Reserve n Import Status Current Serial Applications R	existing Dig v Digipass new Digipa No. lead	ipas App ss fc [0097123456]	ile was imported suc	cessfully.	
	Upgrade e Import nev Reserve n Import Status Current Serial	existing Dig v Digipass new Digipa No. lead	ipas ipas The f App ss fc [ile was imported suc	cessfully.	
	Upgrade e Import new Reserve n Import Status Current Serial Applications R	existing Dig v Digipass vew Digipa No. lead nported	ipas App ss fc [0097123456]	ile was imported suc	APPL 3	

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

🚡 dpmmc - [Console Root\Digipass	Administration\DC1	Digipass]				
🚡 Eile Action Yiew Favorites Y	/indow <u>H</u> elp					<u>_8×</u>
← → 🗈 💽 🗙 🔂 🔮	🖗 🚳 🗰 🝸					
Console Root	Digipass (displaying f	irst 1)				1
 Digipass Administration DC1 		Common second second second second	omain	Digipass Type	Application Names	Application Types
Organizational Unit	Activate Inactival	kg pplication № Change Application pplication	haster	DP300	APPL 1, APPL 2, AP	RO,SG,CR
Assigns the Digipass Application to a Users						

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.

📸 dpmmc - [Console Root\Digip						
Be Action View Favorites ← ⇒ € III × 🛱 Ⅰ	Window Help	-				<u>-8×</u>
	ect User			×		
Dippass Administration Dot Det Cat Det Det	Grace Period (d	ed C No mwards in Organizati ays) 7			ation Names L,APPL 2,AP	Application Types 1 R0,55,CR
	Maximum no. of Search Results User Id	Users to list (1 requi	red) 100 Find			
	testuser		RK Cancel H			
			RKCancelH	eip		

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.

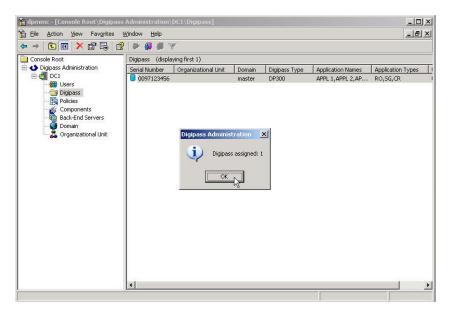


Figure 27: DIGIPASS assignment (4)



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.

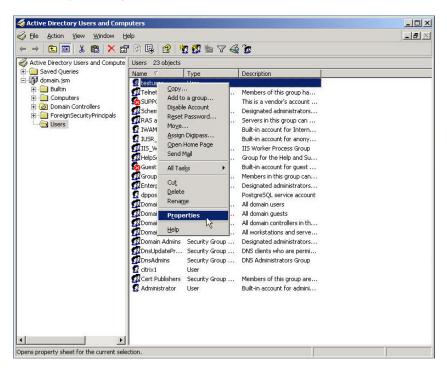


Figure 28: Active Directory User Creation (1)



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.

	Help	그리
	estuser Properties	
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Dulkin Dulkin Computers Dulkin Computers Dulkin ForeignSecurityPrincipal Users	Member Of Dial-in Environment Sessions Remote control Terminal Services Profile CDM+ General Address Account Profile Telephones Organization Image: Digipass User Account Image: Digipass Service Image: Digipass Service Image: Digipass Service Image: Disabled Stored Static Password Image: Disabled Image: Disabled Image: Disabled Authentication Default Image: Disabled Image: Disabled Back:End Authentication Default Image: Disabled Image: Digipass from Another Account Linked User Account Unlink User Account Unlink User Account Image: Disabled	
	Authorization Profiles/Attributes Update History Created On Modified On OK Cancel Apply Help	

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.

Here and Co	mputers	<u>_ ×</u>
🥪 Eile Action Yiew Window	Help	_8×
← → 🗈 🖬 🐰 📾 🗡	estuser Properties	
Active Directory Users and Com Saved Queries South Saved Queries South Saved Save Save Save Save Save Save Save Save	Member Of Dial-in Environment Sessions Remote control Terminal Services Profile COM+ General Address Account Profile Digipass User Account Digipass Assignment Stored Static Password Digipass Assignment New Password Digipass Assignment Authentication Policy Overrides Disabled Local Authentication Default Disabled Back-End Authentication Default Elocal Use Digipass from Another Account Linked User Account Linked User Account. Unlink User Account Link User Account. Unlink User Account Update History Image: Authorization Profiles/Attributes Update History Image: Authorization Profiles/Attributes OK Cancel Apply	
	<u> </u>	

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.

File Action	ry Users and Comp				·미· - 리 2
	Add/Remove Colur	69/	8	6	
Active Director	Large Icons				
+ OI Saved Que	Small Icons			Description	
🗄 🗊 domain. jsrr	List			Description	
🗄 🧰 Builtin	• <u>D</u> etail		Group	Members of this group ha	
🗄 🦲 Compu	Licore Groupe apr	d Computers as conta	and the second se	This is a vendor's account	
🗄 🧭 Domair	Advanced Feature		Group	Designated administrators	
E-C Foreigr	Filter Options		Group	Servers in this group can	
USERS				Built-in account for Intern	
	Customize			Built-in account for anony	
		WPG	Security Group	IIS Worker Process Group	
		HelpServices	Security Group	Group for the Help and Su	
		So Guest	User	Built-in account for guest	
		Group Policy	Security Group	Members in this group can	
		Enterprise A	Security Group	Designated administrators	
		🖸 dppostgres	User	PostgreSQL service account	
		Domain Users	Security Group	All domain users	
		Domain Guests		All domain guests	
		Domain Cont		All domain controllers in th	
		Domain Com	Security Group	All workstations and serve	
		Domain Admins		Designated administrators	
		DnsUpdatePr		DNS clients who are permi	
		2 DnsAdmins	Security Group	DNS Administrators Group	
		🖸 citrix1	User		
			Security Group	Members of this group are	
		🖸 Administrator	User	Built-in account for admini	
	•				
	vanced features and o	hiecto			

Figure 31: Import DIGIPASS (1)

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

🍯 Active Directory	Users and Comp	uters				
🎻 Eile Action <u>V</u>	jew <u>W</u> indow <u>H</u> e	lp				_8×
🗢 🔿 🗈 🚺	🐰 🛍 🗡 😭	1 🗟 😫 🎽	2 📅 🛍 💎 🕯	🧟 ն		
Active Directory L		Digipass-Pool 0 ob	jects			
🗄 🧰 Saved Querie	s	Name 💎	Туре	Description		
🖻 - 🗊 domain. jsm 🕀 🧰 Builtin			T	here are no items to show in th	nis view.	
E Computer	s					
🗄 🧰 Digipass-(
	Pool Delegate Control		1			
🗄 🔛 Digipas	Move	•				
🗄 🧰 Foreigr	Import Digipass					
E LostAn	Digipass Extensity					
😟 🧰 NTDS C		Encryption Settings				
E System	Digipass Extension Find	Iracing				
😟 🚞 Users 💷						
	<u>N</u> ew All Tas <u>k</u> s					
-						
	View		•			
	New Window from	Here	_			
	Cu <u>t</u>					
	<u>D</u> elete Rena <u>m</u> e					
	Refresh					
	Export List					
-	Properties					
	Help					
-						
•						
Imports DPX file(s) to a	current location					

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.

DPX File Browse File C.\Program Files\VASCD\VACMAN Middleware 3\DPX\demo.dpx Browse Key 111111111111111111111111111111111111	ctive Direct	ory User	s and Computers					
File C:\Program Files\WASCD\WACMAN Middleware 3\DPX\demo.dpx Browse Key 111111111111111111111111111111111111	ort Digipass						×	_8
Key 111111111111111111111111111111111111	DPX File						1	
Applications No. Application Name Type Import All Applications 1 APPL 1 RO Import All Applications 2 APPL 2 SG Show Applications 3 APPL 3 CR Import Selected Applications mport Options Import Selected Applications Import Selected Applications Publication rew Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only Monto Selected Applications mport Status Applications Read Applications Read Applications Applications Failed Show Emors	File	C:\Prog	ram Files\VASCO\VACN	IAN Middleware 3\DF	X\demo.dpx	Browse		
Applications No. Application Name Type Import All Applications 1 APPL 1 RO Import All Applications 2 APPL 2 SG Show Applications 3 APPL 3 CR Import Selected Applications mport Options Import Selected Applications Import Selected Applications Publication rew Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only Monto Selected Applications mport Status Applications Read Applications Read Applications Applications Failed Show Emors	Kau	111111		1111111				
1 APPL 1 RO 2 APPL 2 SG 3 APPL 3 CR Import Options Import Selected Applications Import Options Import Selected Applications Reserve new Digipass with activation codes from new DPX file Import selected Applications Reserve new Digipass for individual assignment only mport Status Current Serial No. Application Applications Read Applications Applications Failed Show Errors		Tourn		nunn.	1			
2 APPL 2 SG 3 APPL 3 CR Import Selected Applications mport Options Import new Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only mport Status Current Serial No. Application Applications Read Applications Applications Failed Show Errors	Applications				Import All A			
3 APPL 3 CR Import Selected Applications mport Options Import Selected Applications Upgrade existing Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only Import Selected Application mport Status Import Selection Current Serial No. Application Applications Read Import Status Show Errors Stop					Show An	nlications		
mport Options Upgrade existing Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only mport Status Current Serial No. Applications Read Applications Read Applications Failed Show Errors Stop.						pications		
Upgrade existing Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only moot Status Current Serial No. Applications Read Applications Read Applications Failed Show Enors Stop.					Import Selecte	ed Applications		
Upgrade existing Digipass with activation codes from new DPX file Import new Digipass Applications as inactive Reserve new Digipass for individual assignment only moot Status Current Serial No. Applications Read Applications Read Applications Failed Show Enors Stop.								
Timport new Digipass Applications as inactive Reserve new Digipass for individual assignment only mport Status Current Serial No. Application Applications Read Applications Imported Applications Failed Show Errors Stop	Import Options	·					1	
	Upgrade	existing Di	gipass with activation co	des from new DPX fil	e			
mport Status Current Serial No. Application Applications Read Applications Imported Applications Failed Show Errors	Import ne	w Digipass	s Applications as inactive	,				
mport Status Current Serial No. Applications Read Applications Imported Applications Failed Show Errors	E Beserve i	new Diaipa	ass for individual assignr	nent only				
Current Serial No. Application Application Applications Read Applications Imported Applications Failed Show Errors Stop								
Applications Read Applications Imported Applications Failed Show Errors Stop	Import Status-							
Applications Imported Applications Failed Show Errors Stop	Current Serial	l No.		Application				
Applications Imported Applications Failed Show Errors Stop	Applications (Read	-					
Applications Failed Show Errors Stop		1000	1					
	Applications I	mported						
	Applications F	Failed		Show Error	n Str	. 1		
Close Help			-8			·P'		
				Clos	e H	elp		
				Close	e H	elp		
				Clos	e Hi	elp		

Figure 33: Import DIGIPASS (1)

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

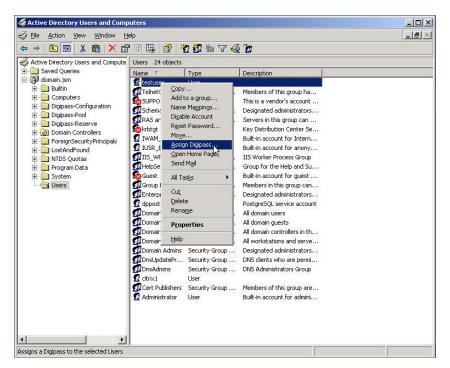
	ory obtain	s and Computers			
ort Digipass					× _8
DPX File	C:\Prog	ram Files\VASCO\VACM	IAN Middlewar	e 3\DPX\demo.dpx Browse	
Key	1111111	11111111111111111111111	1111111		
Applications	No.	Application Name	Туре	Import All Applications	
	1 2 3	APPL 1 APPL 2 APPL 3	RO SG CR	Show Applications	
				Import Selected Applications	
Import Options		gipass with activation co	ideo from nous	DEV 6la	
		7.		DEX IIIE	
		s Applications as inactive ass for individual assignm			
				Digipass Administration	
Reserve r	new Digipa			Digipass Administration	3
Reserve r	new Digipa I No.	ass for individual assignm	nent only		3
Reserve r Import Status - Current Serial	new Digipa INo. Read	oss for individual assignn	nent only		Ī
F Reserve r Import Status – Current Serial Applications F	new Digipa I No. Read Imported	0097123456	nent only Applic		
Reserve r Import Status Current Serial Applications R Applications I	new Digipa I No. Read Imported	ass for individual assignn 0097123456 3 3	nent only Applic	The file was imported successfully. OK WErrors Stop	
Reserve r Import Status Current Serial Applications R Applications I	new Digipa I No. Read Imported	ass for individual assignn 0097123456 3 3	nent only Applic	The file was imported successfully.	
Reserve r Import Status Current Serial Applications R Applications I	new Digipa I No. Read Imported	ass for individual assignn 0097123456 3 3	nent only Applic	The file was imported successfully. OK WErrors Stop	
Reserve r Import Status Current Serial Applications R Applications I	new Digipa I No. Read Imported	ass for individual assignn 0097123456 3 3	nent only Applic	The file was imported successfully. OK WErrors Stop	

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

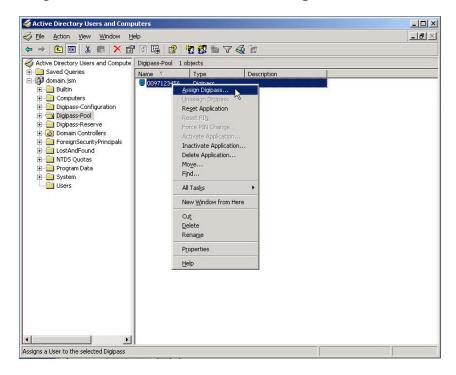


Figure 36: DIGIPASS Assignment (2)



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.

Active Directory Users and Comp Elle Action View Window He	elp				 e
⊨ → 🖻 🖬 👗 💼 🗙 🖆	0 🖪 😫 🎽	3 敬 🐚 🖓 🍕	<u>ت</u>		
🖇 Active Directory Users and Compute	Digipass-Pool 1 ob	jects			
🗄 🛄 Saved Queries 🗄 🚮 domain. jsm	Name 🗸	Туре	Description		
E-Builtin	0097123456	Digipass			
🗈 🦲 Computers	s	elect User			×
Digipass-Configuration Digipass-Pool		- Selection Criteria			
Digipass-Pool Digipass-Reserve		User ID	testuser		_
主 🧭 Domain Controllers		To			
ForeignSecurityPrincipals LostAndFound			I.		
LostAndFound MTDS Quotas		Digipass Assign	ed C No	C Yes C Either	
🖭 🦲 Program Data		Search dow	nwards in Organizatio	onal Unit hierarchy	
		Find and Select Maximum no. of Search Results	Users to list (1 requin	ed) [100 F	ind
		User Id	User Name	Organizational Unit	
		testuser	testuser	Users	
<u> </u>				Cancel H	elp

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.

GajShield VPN Client	
<u>File VPN Configuration View</u>	Tools ?
GAJ SH Security S	HELD Simplified IPSEC VPN CLIENT
🔑 Console	Phase 2 (IPSec Configuration)
🔯 Parameters	Name Tunnel1
😂 Connections	VPN Client address 192 . 168 . 2 . 44
Root S GS_VASCO () () () () () () () () () () () () () (Address type Subnet address Remote LAN address 192 . 168 . 2 . 0 Subnet Mask 255 . 255 . 0
	Encryption 3DES P2 Advanced Authentication MD5 Scripts Mode Tunnel
	PFS Group DH5 (1536) Open Tunnel
	Save & Apply
VPN ready	Tunnel 🥑

Figure 38

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

GajShield VPN Client	L	<u> </u>
File VPN Configuration View	w Tools ?	
GAJ SI Security		C VPN CLIENT
💫 Console	Phase 2 (IPSec Configuration)	
🛞 Paramet 🛞 🚥 🚥	1 Authentication	
	Enter your X-Auth login and password to open the tur Login: testuser Password: xxxxxxx OK Cancel	0 0 Advanced
	Mode Tunnel	
	▼ PFS Group DH5(1536) ▼	Open Tunnel Save & Apply
VPN ready		Tunnel 🥑





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

GajShield VPN Client	
<u>File VPN Configuration View</u>	Tools ?
GAJ SH Security S	
💫 Console	Phase 2 (IPSec Configuration)
Parameters	Name Tunnel1
S Connections	VPN Client address 192 . 168 . 2 . 44
E S Root S S_VASCO C Tunnel1	Address type Subnet address Remote LAN address 192 . 168 . 2 . 0 Subnet Mask 255 . 255 . 0 ESP Encryption 3DES P2 Advanced
	Authentication MD5 Scripts Mode Tunnel
	PFS Group DH5 (1536) Close Tunnel
	Save & Apply
VPN Tunnel opened	Tunnel 🔘

Figure 40



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.

ninistrator Proper	. 5	?
Published Certificate:		I material analysis
· · · · · · · · · · · · · · · · · · ·		Terminal Services Profile
ieneral Address		phones Organization
	igipass User Account	Digipass Assignment
Assigned Digipass		
and the second sec	OP Type Active Applications	
0097123456	OP300 APPL 3 (CR), APPL 2	? (SG), APPL 1 (RO)
		1.1
1-1		
		Manage
Assignment Status-		
Date Assigned	24/08/2006 17:03:35	Assign
Date Assigned	124/00/2000 17:00:00	Assign
Grace Period End	31/08/2006	Unassign
Backup Virtual Digir	Dass	
backup viituai Digip		
Enable BVDP	Default	
Enable BVDP	Default	
	Default	
Enable BVDP	Default	
Enable BVDP Enabled Until	Default	

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.

dpmmc - [Console Root\Digipass Admini	stration\CSG\Users]				
File Action View Favorites Window					_ 8
🚞 Console Root 🗄 🕁 Digipass Administration	Users (displaying first 2)				
CSG		zational Unit Domain	User Name	Assigned Digipass	
Users	e admin vascodemo	master master			
🗞 Digipass	Vascodemo	master			
Components					

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.

Domain	naster		(Master Domain)
Organizational Unit			
Privileges Available:		Privileges Held:	
Administrative Logon Access Data in All Dc Live Audit Connection View User Create User Update User Delete User Link User Unink User Work Dignes Set Administrative F Set Administrative F Set Administrative F View Digness Delete Digness Delete Digness Create Digness Applic Set Digness Applic Set Digness Set Creater Set Administrative F Reset Digness Applic	rivileges	>> < <<	

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.