THE AUTHENTICATION COMPANY

DIGIPASS Authentication for Fortigate

With Vasco VACMAN Middleware 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

Table of Contents

1 Overview

The purpose of this document is to demonstrate how to configure VACMAN Middleware 3.0 (VM) to work with a Fortigate device. Authentication is arranged on one central place where it can be used in a regular VPN or SSL/VPN connection.

2 Problem Description

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

3 Solution

After configuring VACMAN Middleware and Fortigate 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.

In this integration guide we will make use of a Fortigate 50A. This combines a firewall, an IPSec, PPTP or SSL/VPN and a UTM suite in one. For authentication, we focused on the SSL/VPN part.

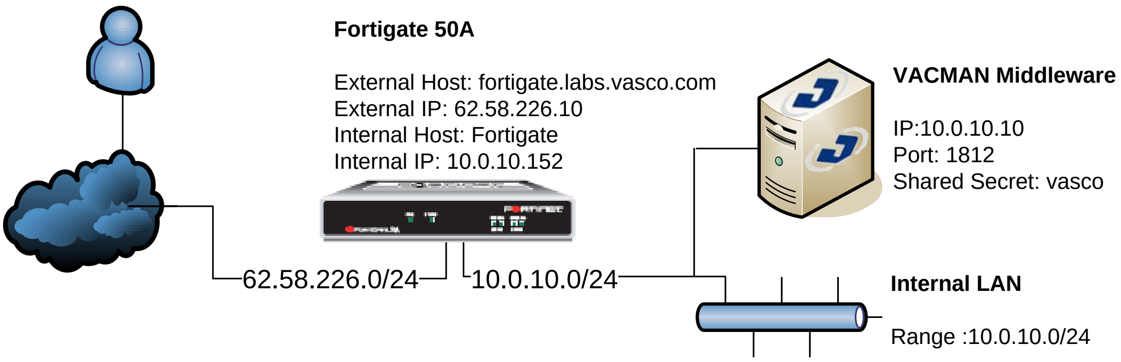


Figure 1: Solution

4 Technical Concept

4.1 General overview

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

4.2 Fortigate prerequisites

Please make sure you have a working setup of the Fortigate. It is very important this is working correctly before you start implementing the authentication to the VM.

Currently all Fortigate devices use the same web config and CLI interface. This means our integration guide is suited for the complete product range of Fortigate devices.

4.3 VACMAN Middleware Prerequisites

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

5 Fortigate Configuration

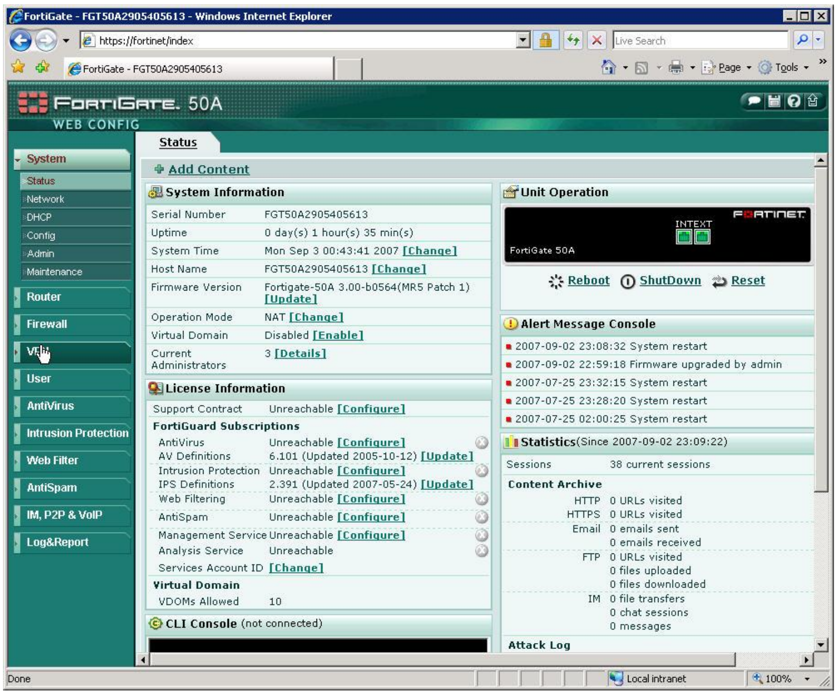
The Fortigate device is configured by web config or by CLI, there is even a CLI window available in the web config screen.

By default the web config is reachable by https://<IP_OR_NAME_Fortigate>.

In our case this becomes: https://Fortigate

5.1 SSL/VPN configuration

In the web config menu, select the **VPN** main category.



System Information

Serial Number	FGT50A2905405613
Uptime	0 day(s) 1 hour(s) 35 min(s)
System Time	Mon Sep 3 00:43:41 2007 [Change]
Host Name	FGT50A2905405613 [Change]
Firmware Version	Fortigate-50A 3.00-b0564(MR5 Patch 1) [Update]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	3 [Details]

License Information

Support Contract	Unreachable [Configure]
FortiGuard Subscriptions	
AntiVirus	Unreachable [Configure]
AV Definitions	6.101 (Updated 2005-10-12) [Update]
Intrusion Protection	Unreachable [Configure]
IPS Definitions	2.391 (Updated 2007-05-24) [Update]
Web Filtering	Unreachable [Configure]
AntiSpam	Unreachable [Configure]
Management Service	Unreachable [Configure]
Analysis Service	Unreachable
Services Account ID	[Change]
Virtual Domain	
VDOMs Allowed	10

CLI Console (not connected)

Unit Operation

Alert Message Console

- 2007-09-02 23:08:32 System restart
- 2007-09-02 22:59:18 Firmware upgraded by admin
- 2007-07-25 23:32:15 System restart
- 2007-07-25 23:28:20 System restart
- 2007-07-25 02:00:25 System restart

Statistics(Since 2007-09-02 23:09:22)

Sessions	38 current sessions
Content Archive	
HTTP	0 URLs visited
HTTPS	0 URLs visited
Email	0 emails sent 0 emails received
FTP	0 URLs visited 0 files uploaded 0 files downloaded
IM	0 file transfers 0 chat sessions 0 messages
Attack Log	

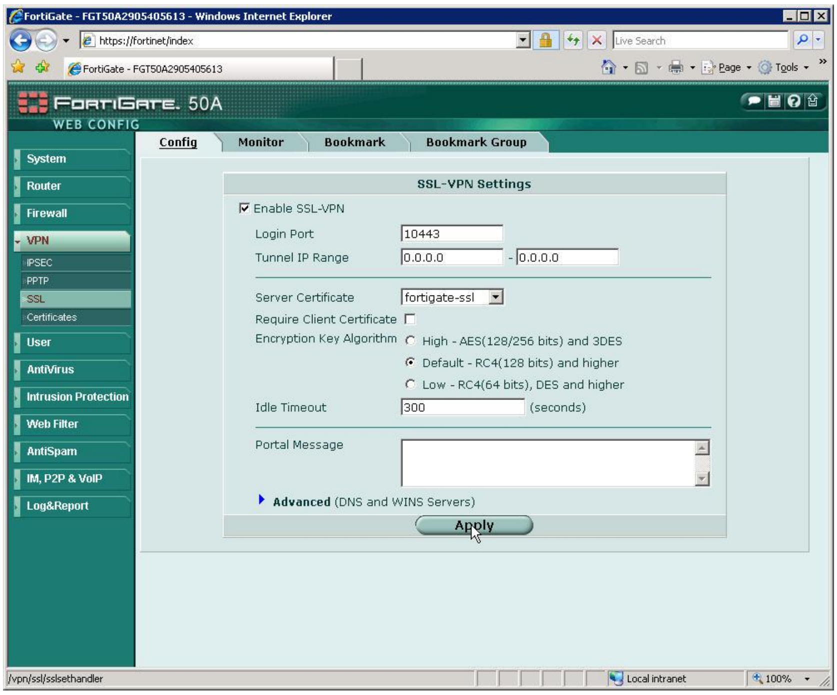
Figure 2: SSL/VPN configuration (1)

Select the **SSL** sub category.

Select the **Enable SSL-VPN** box.

If necessary you can select another ‘Server Certificate’ or a ‘Tunnel IP Range’, if you want to allow client to create a VPN-tunnel.

Click **Apply** to continue.



SSL-VPN Settings

☑ Enable SSL-VPN

Login Port: 10443

Tunnel IP Range: 0.0.0.0 - 0.0.0.0

Server Certificate: fortigate-ssl

Require Client Certificate □

Encryption Key Algorithm:
○ High - AES(128/256 bits) and 3DES
● Default - RC4(128 bits) and higher
○ Low - RC4(64 bits), DES and higher

Idle Timeout: 300 (seconds)

Portal Message

Advanced (DNS and WINS Servers)

Figure 3: SSL/VPN configuration (3)

5.2 RADIUS configuration

Go to the **User** main category and select **RADIUS** as sub category.
Click the **Create New** button to add a new RADIUS connection.

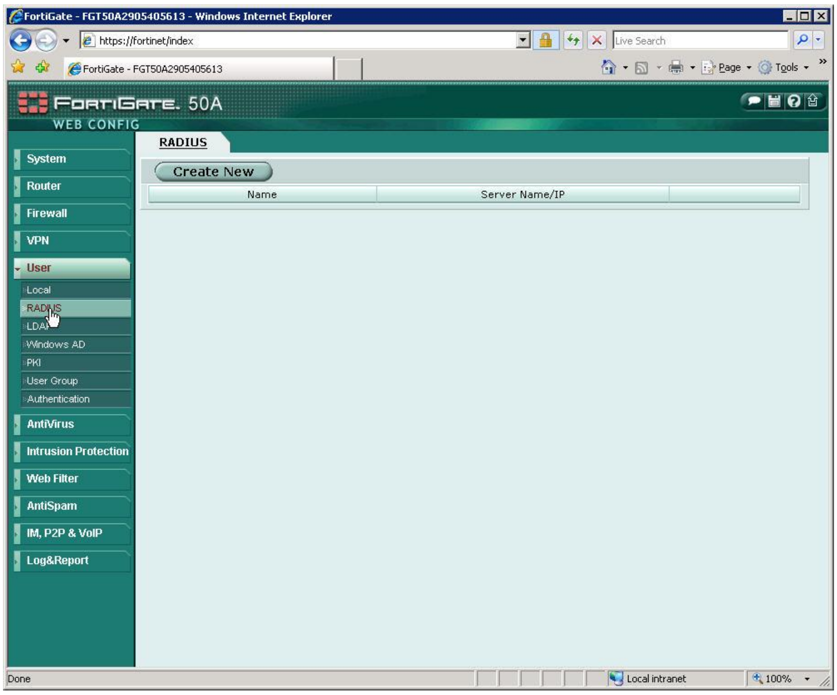
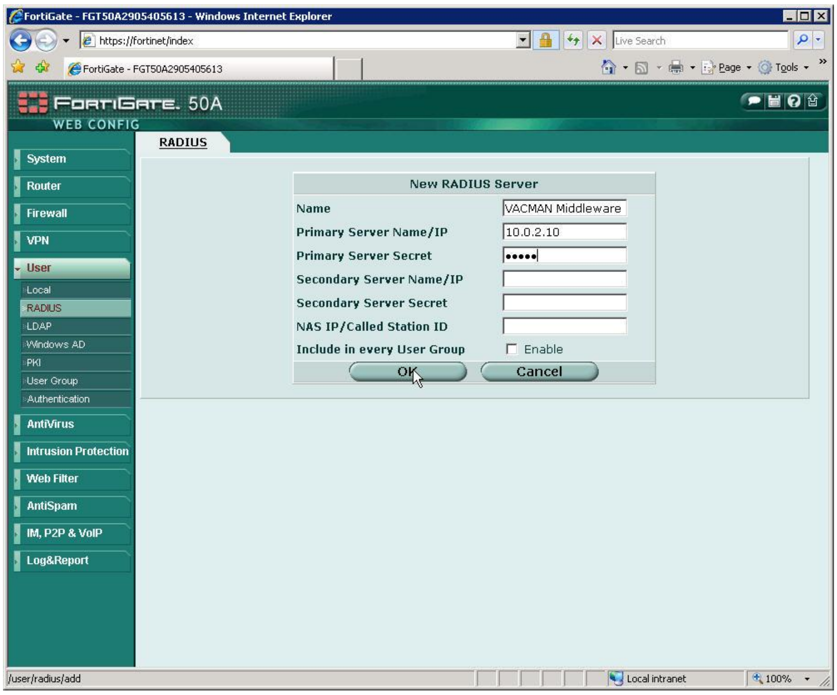


Figure 4: RADIUS configuration (1)

Fill in the **Name** and **Primary Server Name/IP** and **Primary Server Secret**.
If you necessary you can add a secondary server as well, but this is not required to continue. Click **OK** to create the RADIUS server.



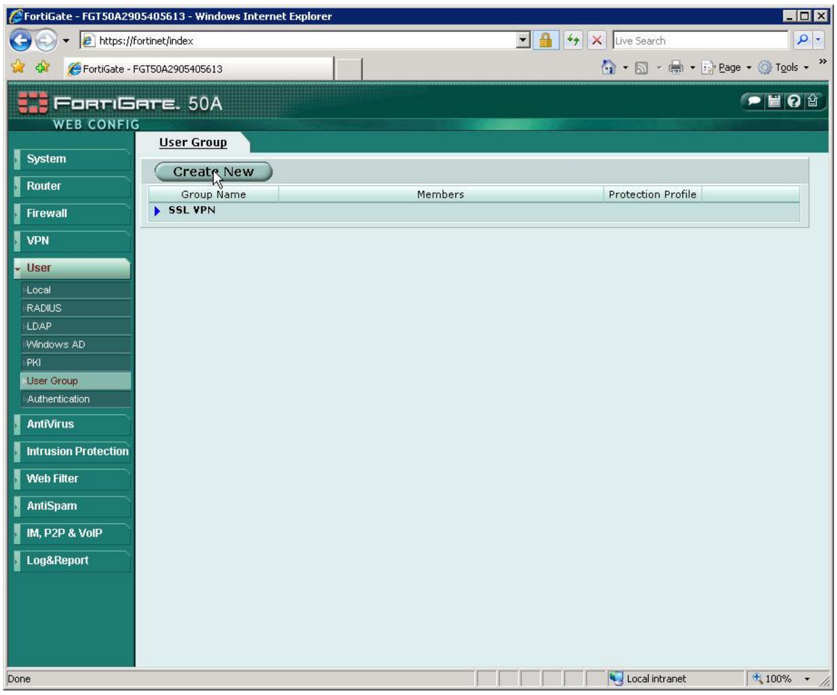
New RADIUS Server

Name	VACMAN Middleware
Primary Server Name/IP	10.0.2.10
Primary Server Secret	•••••
Secondary Server Name/IP	
Secondary Server Secret	
NAS IP/Called Station ID	
Include in every User Group	□ Enable

Figure 5: RADIUS configuration (2)

5.3 Group configuration

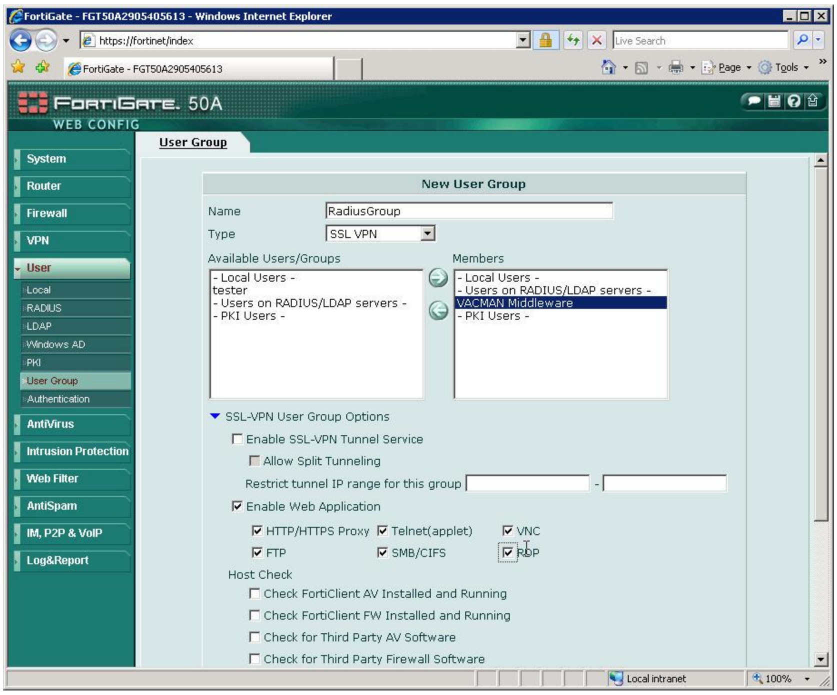
We will now create a group to use in the firewall rules. Click on the User main category, select **User Group** as sub category and click the **Create New** button.



Group Name	Members	Protection Profile
SSL VPN		

Figure 6: Group configuration (1)

Enter a Name and select SSL VPN as type. Select in the left column the **RADIUS server** you created earlier and click on the ➔ button to get in the right column. If necessary click on the **SSL-VPN User Group Options** for more options. Here you can enable tunneling options and enable web applications. Click **OK** to create this group.



New User Group

Name: RadiusGroup

Type: SSL VPN

Available Users/Groups:
- Local Users -
tester
- Users on RADIUS/LDAP servers -
- PKI Users -

Members:
- Local Users -
- Users on RADIUS/LDAP servers -
VACMAN Middleware
- PKI Users -

SSL-VPN User Group Options

☐ Enable SSL-VPN Tunnel Service

☐ Allow Split Tunneling

Restrict tunnel IP range for this group ____ - ____

☑ Enable Web Application

☑ HTTP/HTTPS Proxy ☑ Telnet(applet) ☑ VNC

☑ FTP ☑ SMB/CIFS ☑ RDP

Host Check

☐ Check FortiClient AV Installed and Running

☐ Check FortiClient FW Installed and Running

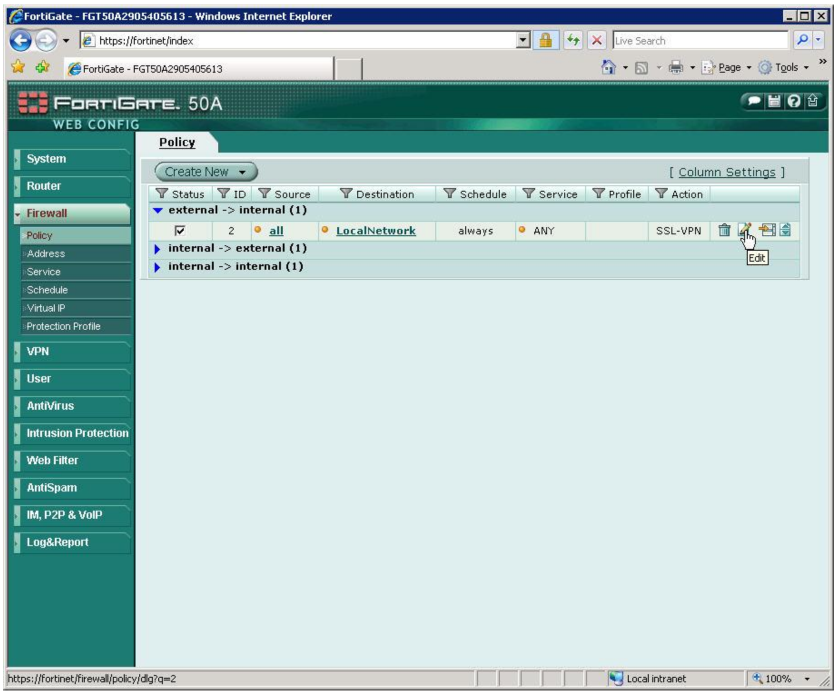
☐ Check for Third Party AV Software

☐ Check for Third Party Firewall Software

Figure 7: Group configuration (2)

5.4 Firewall configuration

To enable SSL-VPN we have to create also a firewall policy allowing connection from the VPN side to the internal network. To do so, click the **Firewall** main category and select **Policy** as sub category. Click the **Create New** button.



Status	ID	Source	Destination	Schedule	Service	Profile	Action
external -> internal (1)							
☑	2	all	LocalNetwork	always	ANY		SSL-VPN
internal -> external (1)							
internal -> internal (1)							

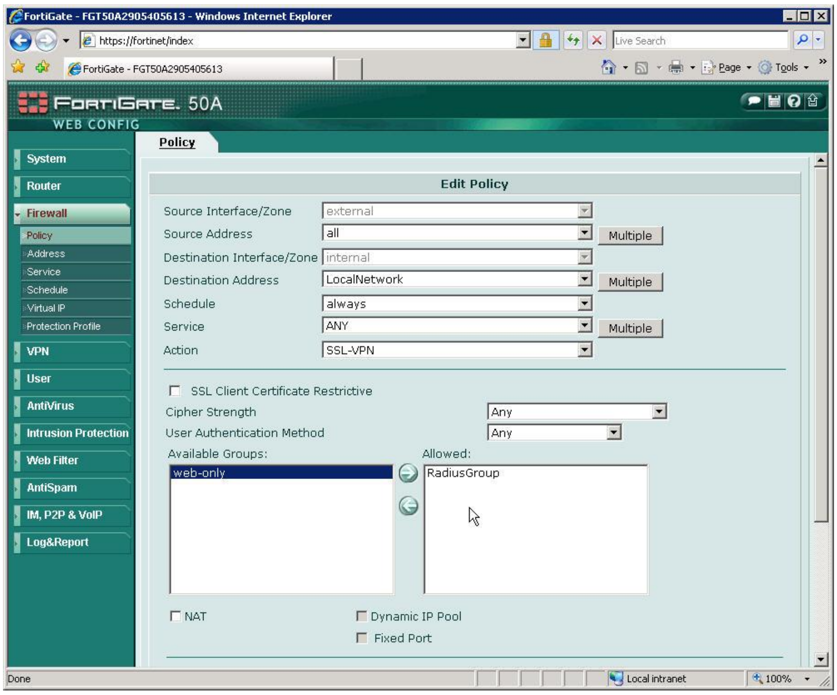
Figure 8: Firewall configuration (1)

The following settings are used for an SSL-VPN connection:

• Source Interface/Zone	external
• Source Address	all
• Destination Interface/Zone	internal
• Destination Address	LocalNetwork
• Shedule	always
• Service	ANY
• Action	SSL-VPN

From the ‘Available Groups’ window, select the **RADIUS group** and click the ➔ button to transfer the group to the Allowed window.

To finish, click on the **OK** button in the bottom of the screen.



Edit Policy

Source Interface/Zone: external
Source Address: all
Destination Interface/Zone: internal
Destination Address: LocalNetwork
Schedule: always
Service: ANY
Action: SSL-VPN

□ SSL Client Certificate Restrictive
Cipher Strength: Any
User Authentication Method: Any
Available Groups: web-only
Allowed: RadiusGroup

□ NAT
□ Dynamic IP Pool
□ Fixed Port

Figure 9: Firewall configuration (2)

This concludes the configuration of the Fortigate device. The incoming request from the SSL-VPN service will now be handled by the VACMAN Middleware. In the next chapters we will show how to configure VM and how to assign a DIGIPASS to a user.

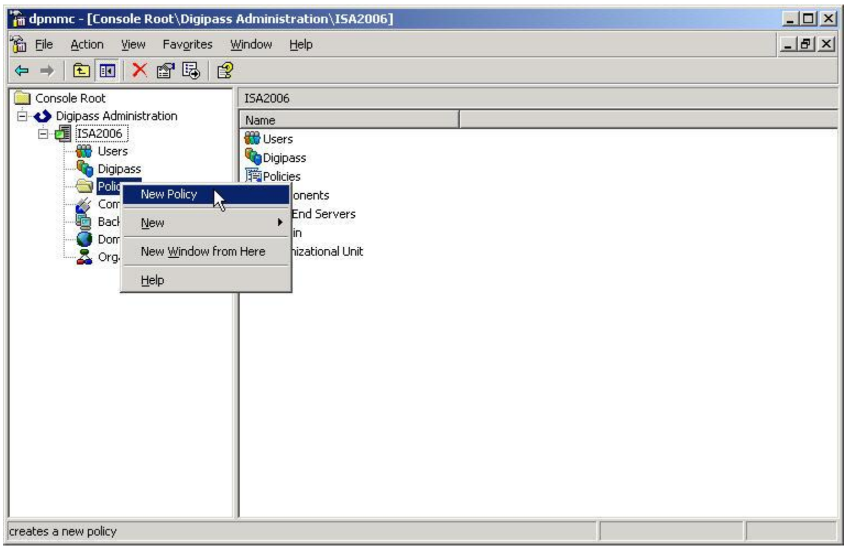
In the chapter after those we will test the Fortigate setup with a response only and a challenge/response DIGIPASS.

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**.

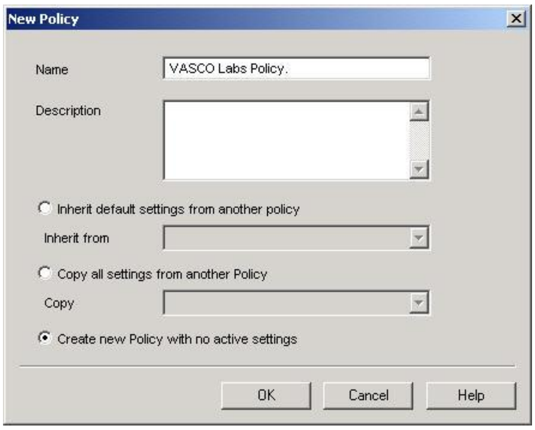


creates a new policy

Figure 10: 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:

○ Inherit default settings from another policy

Inherit from:

○ Copy all settings from another Policy

Copy:

● Create new Policy with no active settings

Figure 11: VM configuration (2)

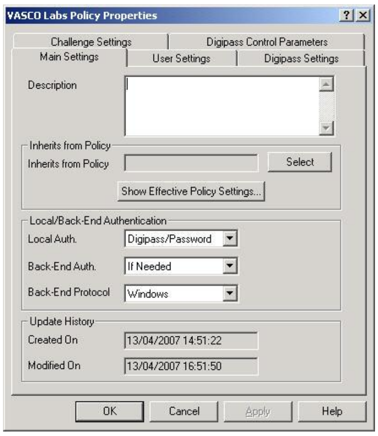
We chose to create a new policy and specify all details about the authentication policy.

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
  - 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.


VASCO Labs Policy Properties

Main Settings

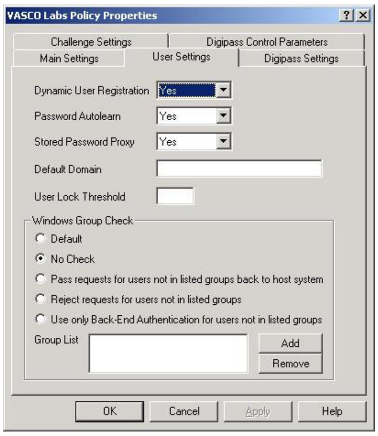
Description:

Inherits from Policy:

Local/Back-End Authentication
Local Auth.: Digipass/Password
Back-End Auth.: If Needed
Back-End Protocol: Windows

Update History
Created On: 13/04/2007 14:51:22
Modified On: 13/04/2007 16:51:50

Figure 12: VM configuration (3)

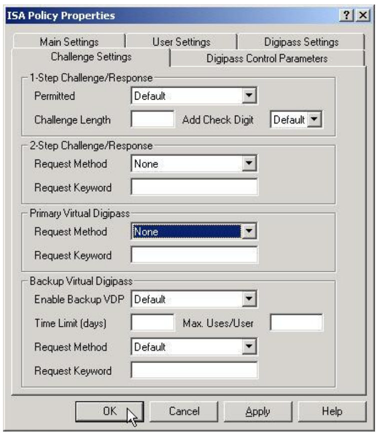

VASCO Labs Policy Properties

User Settings

Dynamic User Registration: Yes
Password Autolearn: Yes
Stored Password Proxy: Yes
Default Domain:
User Lock Threshold:

Windows Group Check
○ Default
● No Check
○ Pass requests for users not in listed groups back to host system
○ Reject requests for users not in listed groups
○ Use only Back-End Authentication for users not in listed groups
Group List:

Figure 13: VM configuration (4)


ISA Policy Properties

Challenge Settings

1-Step Challenge/Response
Permitted: Default
Challenge Length: Add Check Digit: Default

2-Step Challenge/Response
Request Method: None
Request Keyword:

Primary Virtual Digipass
Request Method: None
Request Keyword:

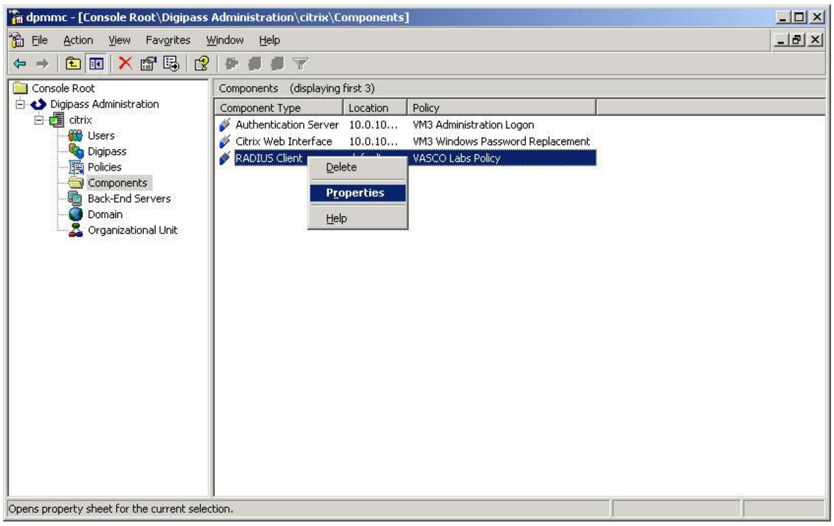
Backup Virtual Digipass
Enable Backup VDP: Default
Time Limit (days): Max. Uses/User:
Request Method: Default
Request Keyword:

Figure 14: 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.

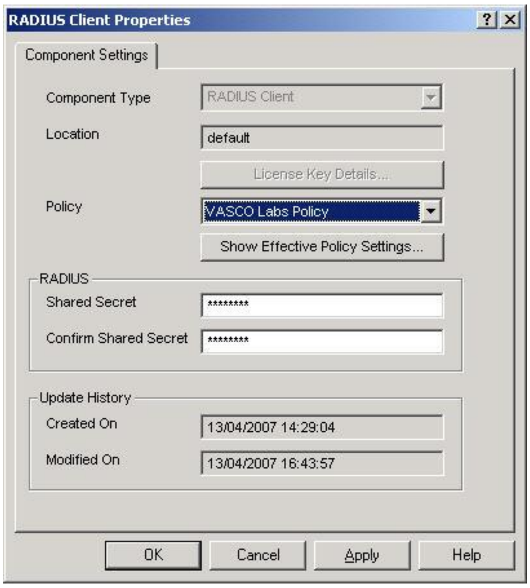

dpmmc - [Console Root\Digipass Administration\citrix\Components]
File Action View Favorites Window Help
Console Root
Digipass Administration
citrix
Users
Digipass
Policies
Components
Back-End Servers
Domain
Organizational Unit
Delete
Properties
Help
Opens property sheet for the current selection.

Components (displaying first 3)

Component Type	Location	Policy
Authentication Server	10.0.10...	VM3 Administration Logon
Citrix Web Interface	10.0.10...	VM3 Windows Password Replacement
RADIUS Client	default	VASCO Labs Policy

Figure 15: 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

Policy: VASCO Labs Policy

RADIUS

Shared Secret: ********

Confirm Shared Secret: ********

Update History

Created On: 13/04/2007 14:29:04

Modified On: 13/04/2007 16:43:57

Figure 16: 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

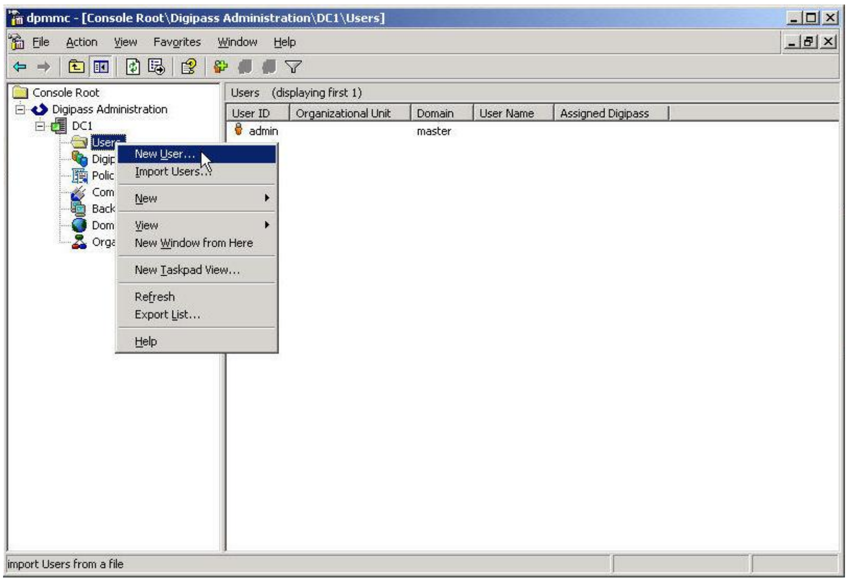
The **user creation** steps you will find in this chapter are optional when you didn't activate the option **Dynamic User Registration (DUR) and/or Password Autolearn** in your policy settings.

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

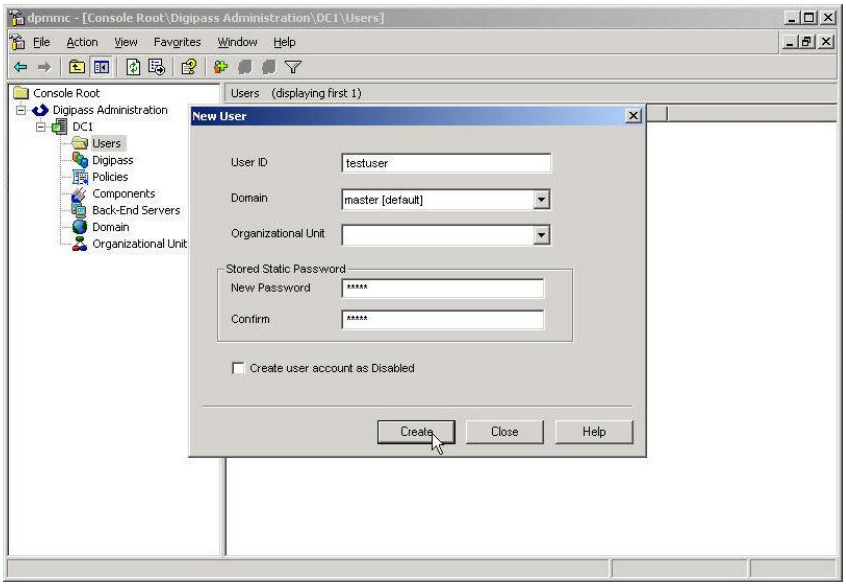
User creation, while using an ODBC back-end, will happen in the DIGIPASS Administration MMC. Right-click the Users folder and select **New User ...**.



User ID	Organizational Unit	Domain	User Name	Assigned Digipass
admin		master		

Figure 17: ODBC User Creation (1)

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



User ID: testuser

Domain: master [default]

Organizational Unit:

Stored Static Password

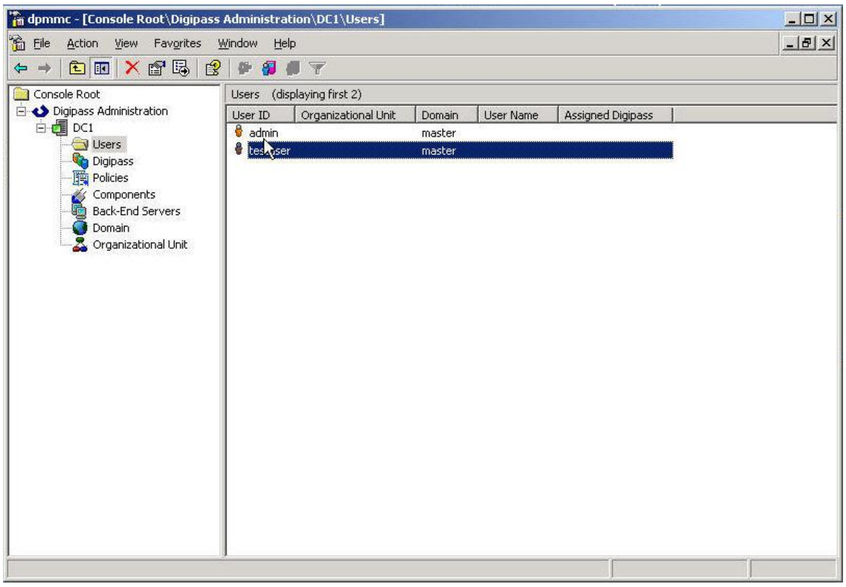
New Password: *****

Confirm: *****

☐ Create user account as Disabled

Figure 18: 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.



Users (displaying first 2)

User ID	Organizational Unit	Domain	User Name	Assigned Digipass
admin		master		
testuser		master		

Figure 19: ODBC User Creation (3)

7.1.2 Import DIGIPASS

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

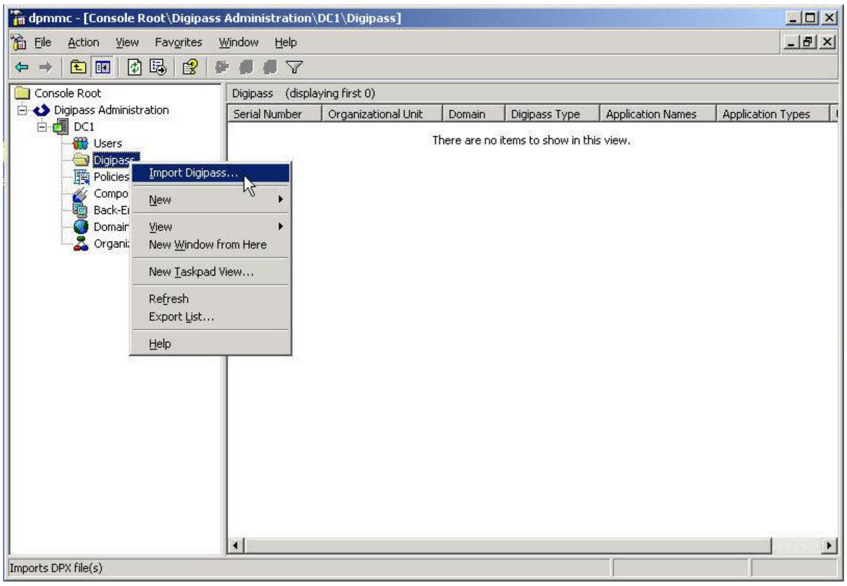
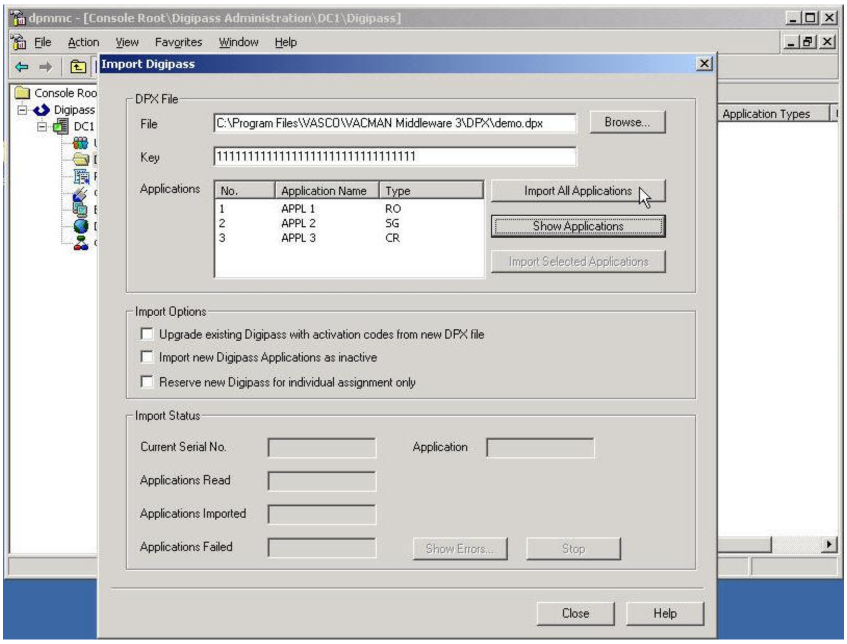


Figure 20: Import DIGIPASS (1)

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.



File: C:\Program Files\VASCO\VACMAN Middleware 3\DPX\demo.dpx

Key: 11111111111111111111111111111111

Applications:

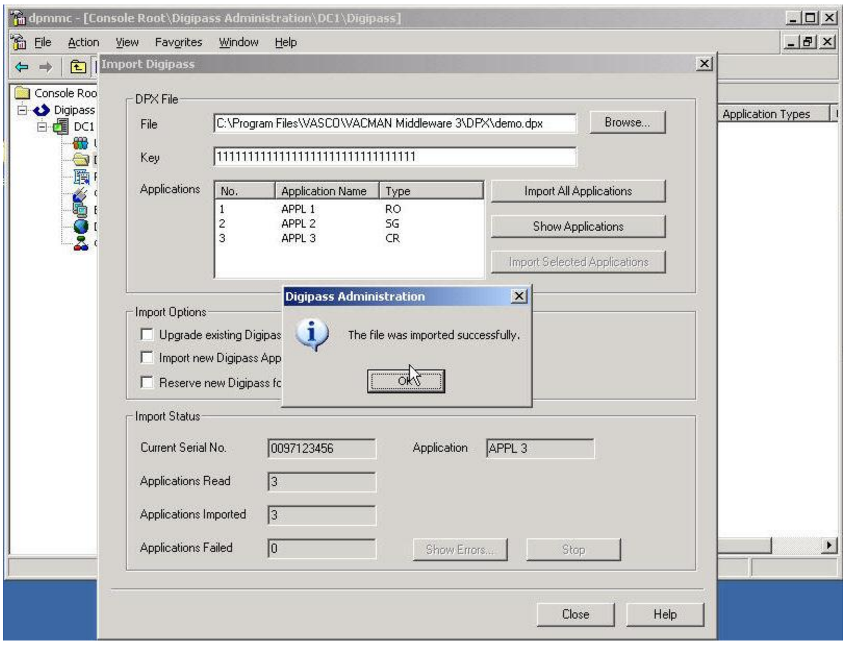
No.	Application Name	Type
1	APPL 1	RO
2	APPL 2	SG
3	APPL 3	CR

☐ Upgrade existing Digipass with activation codes from new DPX file
☐ Import new Digipass Applications as inactive
☐ Reserve new Digipass for individual assignment only

Current Serial No.
Application
Applications Read
Applications Imported
Applications Failed

Figure 21: Import DIGIPASS (2)

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



File: C:\Program Files\VASCO\VACMAN Middleware 3\DPX\demo.dpx

Key: 11111111111111111111111111111111

No.	Application Name	Type
1	APPL 1	RO
2	APPL 2	SG
3	APPL 3	CR

□ Upgrade existing Digipas

□ Import new Digipass App

□ Reserve new Digipass fo

The file was imported successfully.

Current Serial No.: 0097123456

Application: APPL 3

Applications Read: 3

Applications Imported: 3

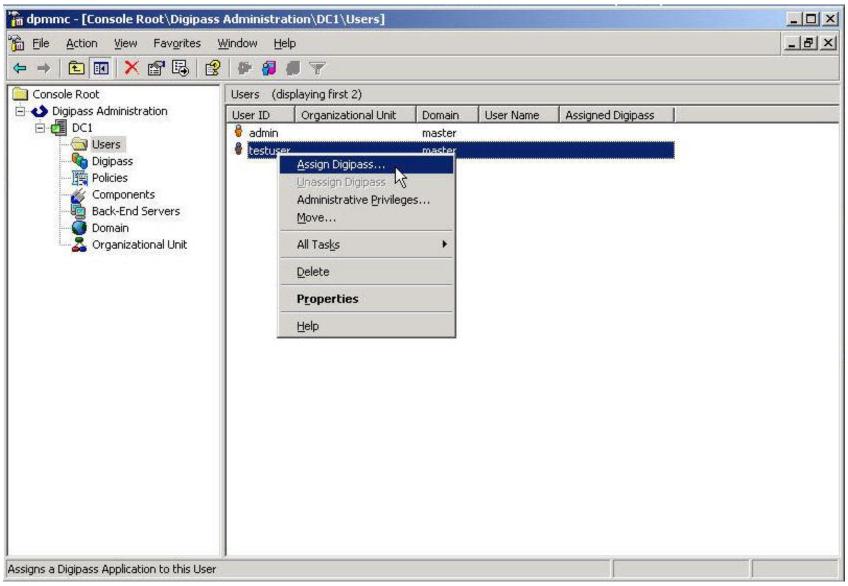
Applications Failed: 0

Figure 22: 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 …

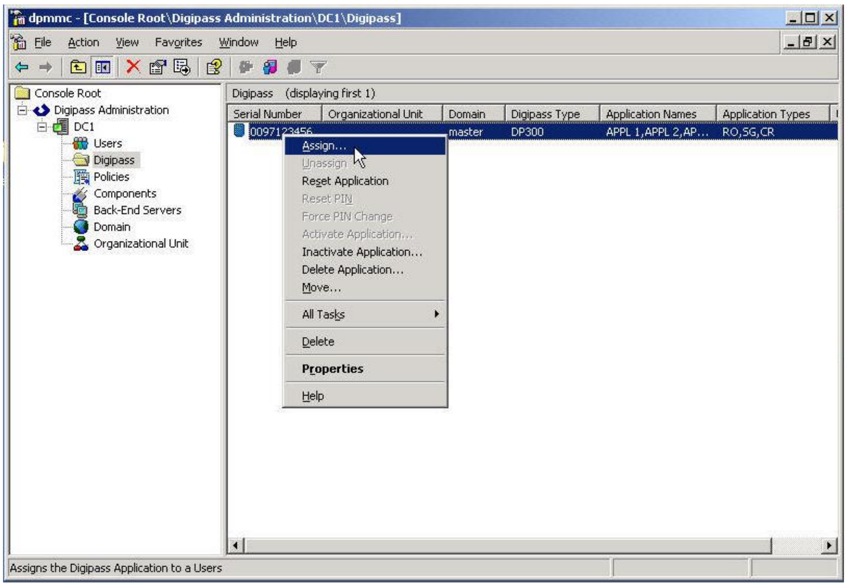


User ID	Organizational Unit	Domain	User Name	Assigned Digipass
admin		master		
testuser		master		

Assigns a Digipass Application to this User

Figure 23: DIGIPASS assignment (1)

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



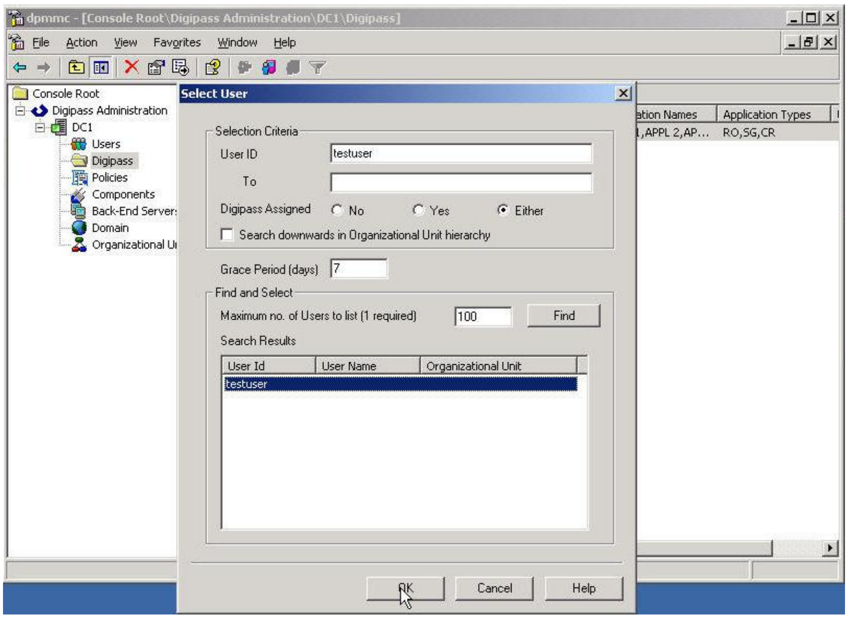
Serial Number	Organizational Unit	Domain	Digipass Type	Application Names	Application Types
0097123456		master	DP300	APPL 1,APPL 2,AP…	RO,SG,CR

Assigns the Digipass Application to a Users

Figure 24: 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.



Selection Criteria

User ID: testuser

To:

Digipass Assigned ○ No ○ Yes ● Either

□ Search downwards in Organizational Unit hierarchy

Grace Period (days) 7

Find and Select

Maximum no. of Users to list (1 required) 100 Find

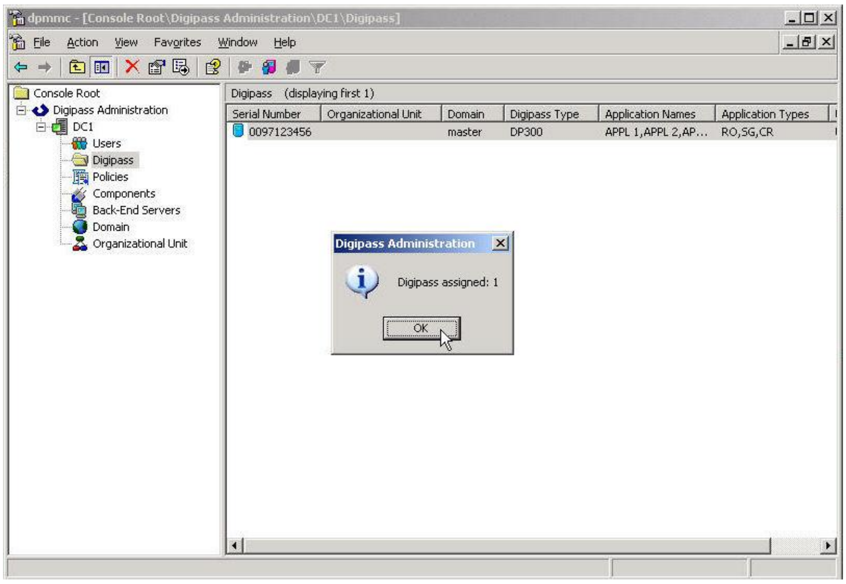
Search Results

User Id	User Name	Organizational Unit
testuser		

Figure 25: 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.



Digipass (displaying first 1)

Serial Number	Organizational Unit	Domain	Digipass Type	Application Names	Application Types
0097123456		master	DP300	APPL 1,APPL 2,AP...	RO,SG,CR

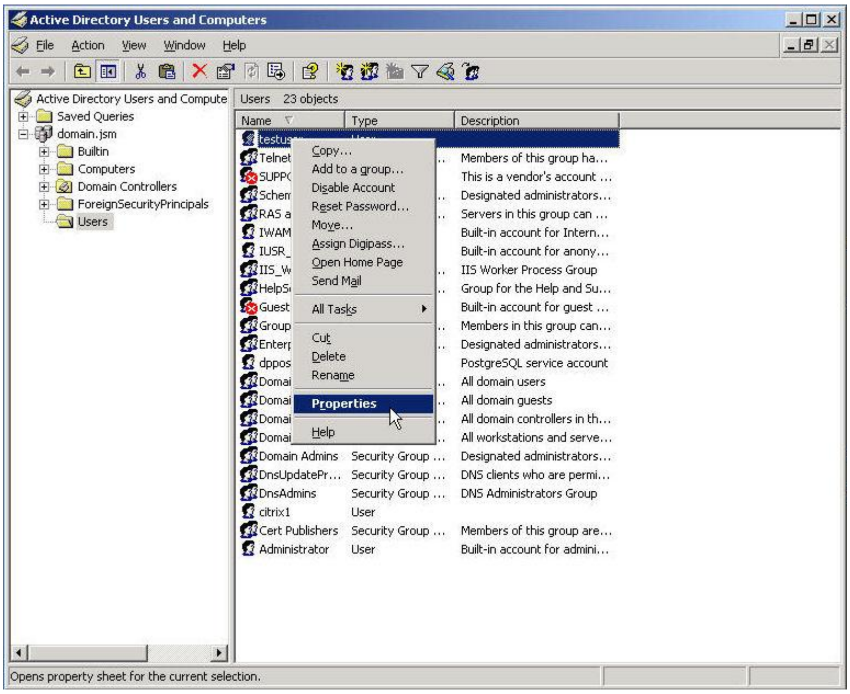
Digipass assigned: 1

Figure 26: 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.

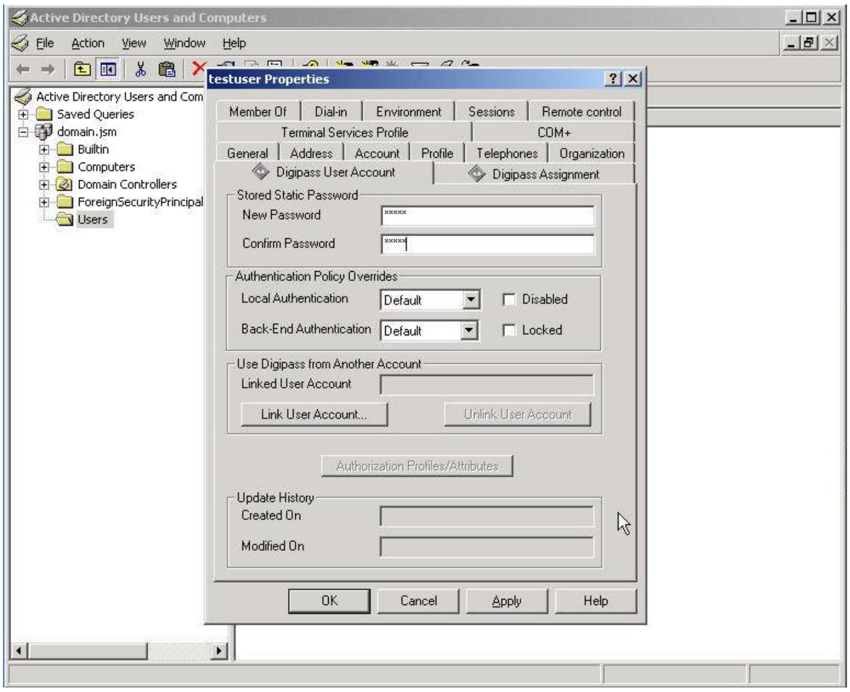


Name	Type	Description
testus		
Telnet	..	Members of this group ha...
SUPPC		This is a vendor's account ...
Schem	..	Designated administrators...
RAS a	..	Servers in this group can ...
IWAM		Built-in account for Intern...
IUSR_		Built-in account for anony...
IIS_W	..	IIS Worker Process Group
HelpS	..	Group for the Help and Su...
Guest		Built-in account for guest ...
Group	..	Members in this group can...
Enterp	..	Designated administrators...
dppos		PostgreSQL service account
Domai	..	All domain users
Domai	..	All domain guests
Domai	..	All domain controllers in th...
Domai	..	All workstations and serve...
Domain Admins	Security Group ...	Designated administrators...
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
DnsAdmins	Security Group ...	DNS Administrators Group
citrix1	User	
Cert Publishers	Security Group ...	Members of this group are...
Administrator	User	Built-in account for admini...

Opens property sheet for the current selection.

Figure 27: 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.



Stored Static Password

New Password: *****

Confirm Password: *****

Authentication Policy Overrides

Local Authentication: Default ☐ Disabled

Back-End Authentication: Default ☐ Locked

Use Digipass from Another Account

Linked User Account:

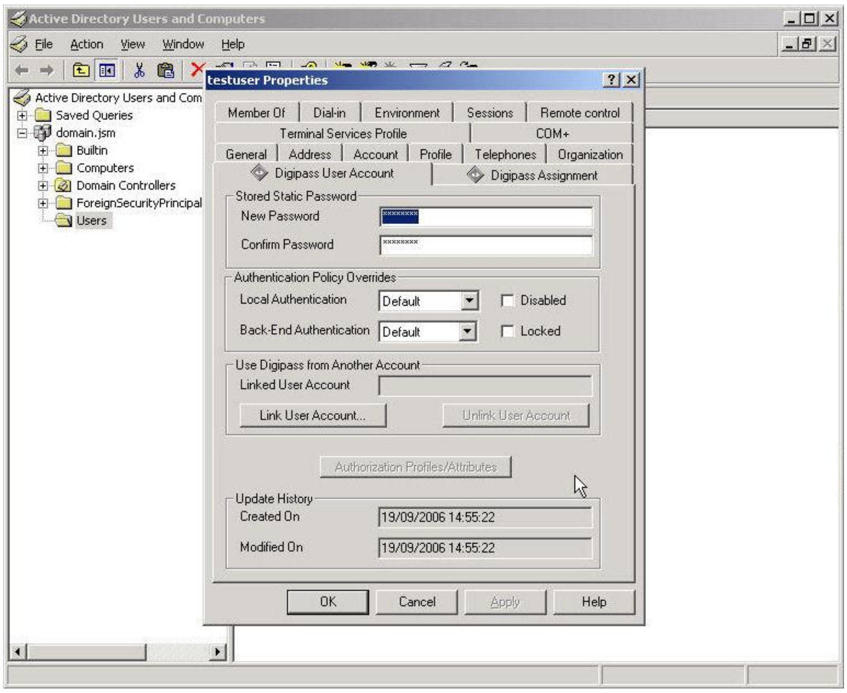
Update History

Created On:

Modified On:

Figure 28: 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.



Stored Static Password

New Password: ********

Confirm Password: ********

Authentication Policy Overrides

Local Authentication: Default ☐ Disabled

Back-End Authentication: Default ☐ Locked

Use Digipass from Another Account

Linked User Account:

Update History

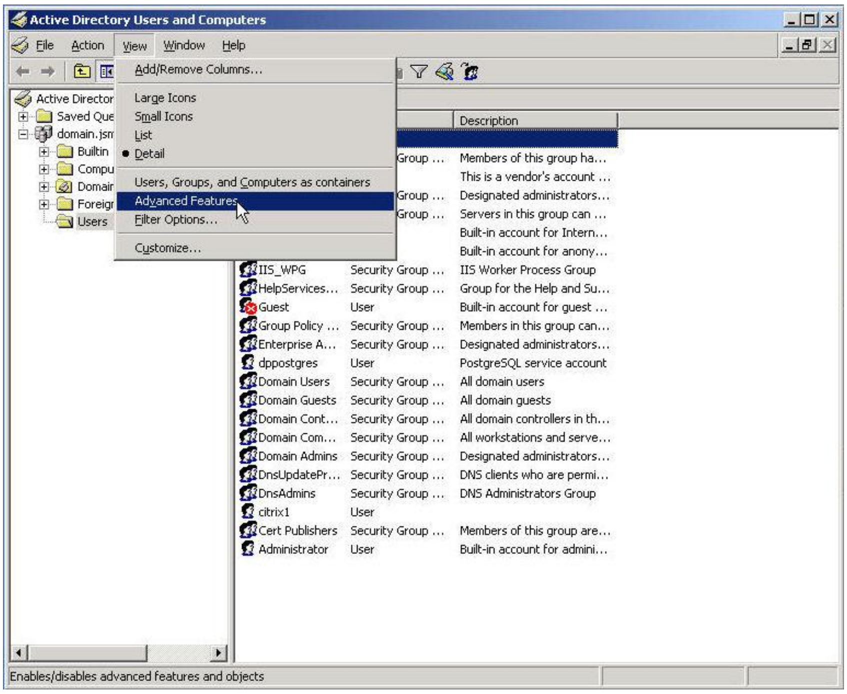
Created On: 19/09/2006 14:55:22

Modified On: 19/09/2006 14:55:22

Figure 29: 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.

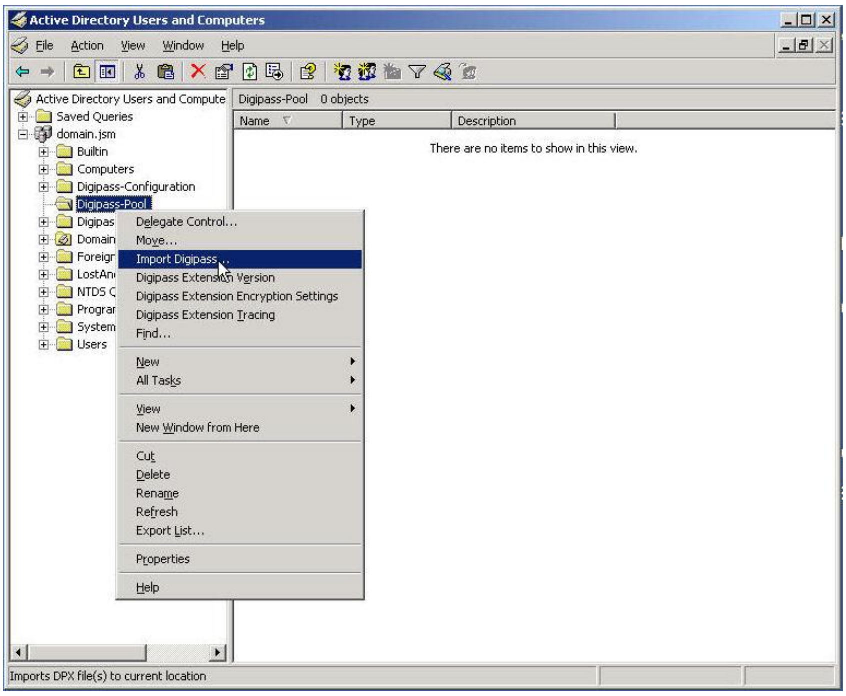


		Description
	Group ...	Members of this group ha...
		This is a vendor's account ...
	Group ...	Designated administrators...
	Group ...	Servers in this group can ...
		Built-in account for Intern...
		Built-in account for anony...
IIS_WPG	Security Group ...	IIS Worker Process Group
HelpServices...	Security Group ...	Group for the Help and Su...
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	Security Group ...	All domain guests
Domain Cont...	Security Group ...	All domain controllers in th...
Domain Com...	Security Group ...	All workstations and serve...
Domain Admins	Security Group ...	Designated administrators...
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
DnsAdmins	Security Group ...	DNS Administrators Group
citrix1	User	
Cert Publishers	Security Group ...	Members of this group are...
Administrator	User	Built-in account for admini...

Enables/disables advanced features and objects

Figure 30: Import DIGIPASS (1)

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

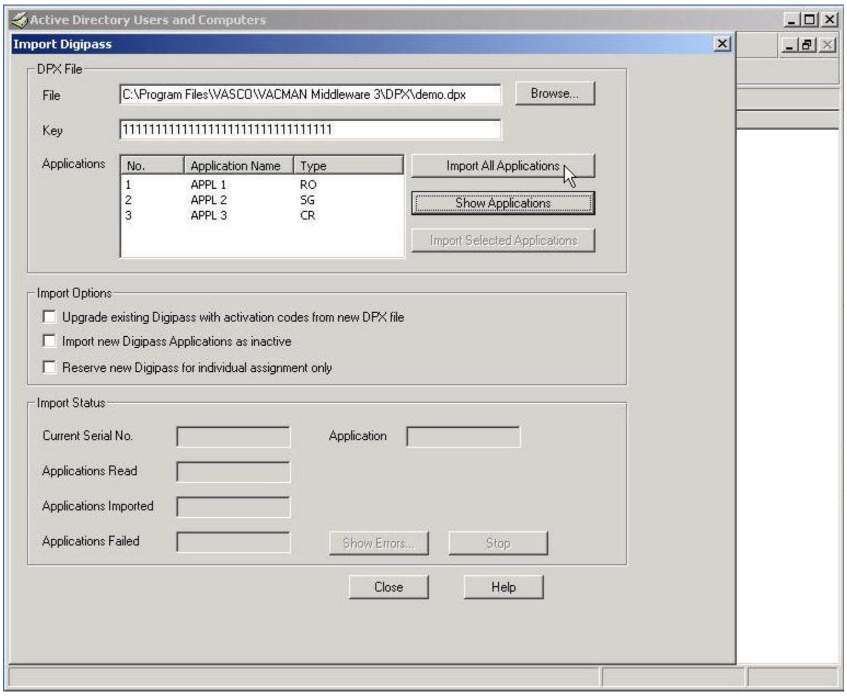


There are no items to show in this view.

Imports DPX file(s) to current location

Figure 31: 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.



File: C:\Program Files\VASCO\VACMAN Middleware 3\DPX\demo.dpx

Key: 11111111111111111111111111111111

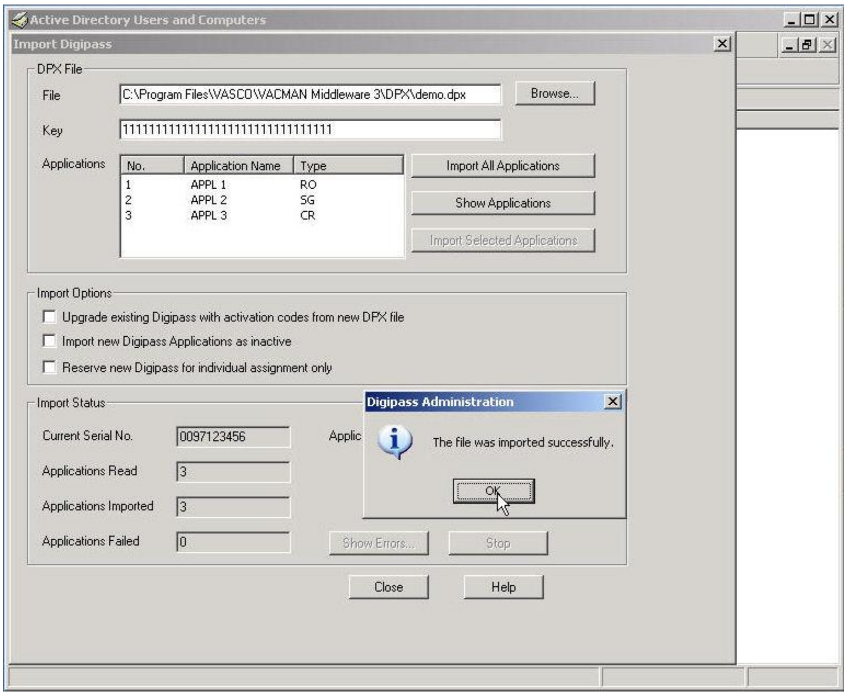
No.	Application Name	Type
1	APPL 1	RO
2	APPL 2	SG
3	APPL 3	CR

- □ Upgrade existing Digipass with activation codes from new DPX file
- □ Import new Digipass Applications as inactive
- □ Reserve new Digipass for individual assignment only

Current Serial No.:
Application:
Applications Read:
Applications Imported:
Applications Failed:

Figure 32: Import DIGIPASS (1)

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



File: C:\Program Files\VASCO\VACMAN Middleware 3\DPX\demo.dpx

Key: 11111111111111111111111111111111

No.	Application Name	Type
1	APPL 1	RO
2	APPL 2	SG
3	APPL 3	CR

- □ Upgrade existing Digipass with activation codes from new DPX file
- □ Import new Digipass Applications as inactive
- □ Reserve new Digipass for individual assignment only

Current Serial No.: 0097123456
Applic
Applications Read: 3
Applications Imported: 3
Applications Failed: 0

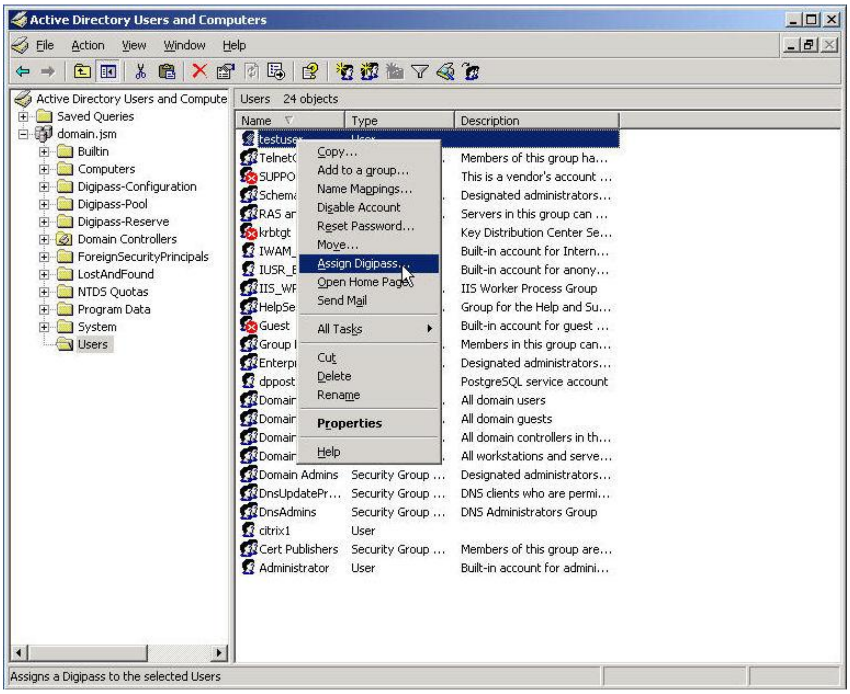
The file was imported successfully.

Figure 33: 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 …

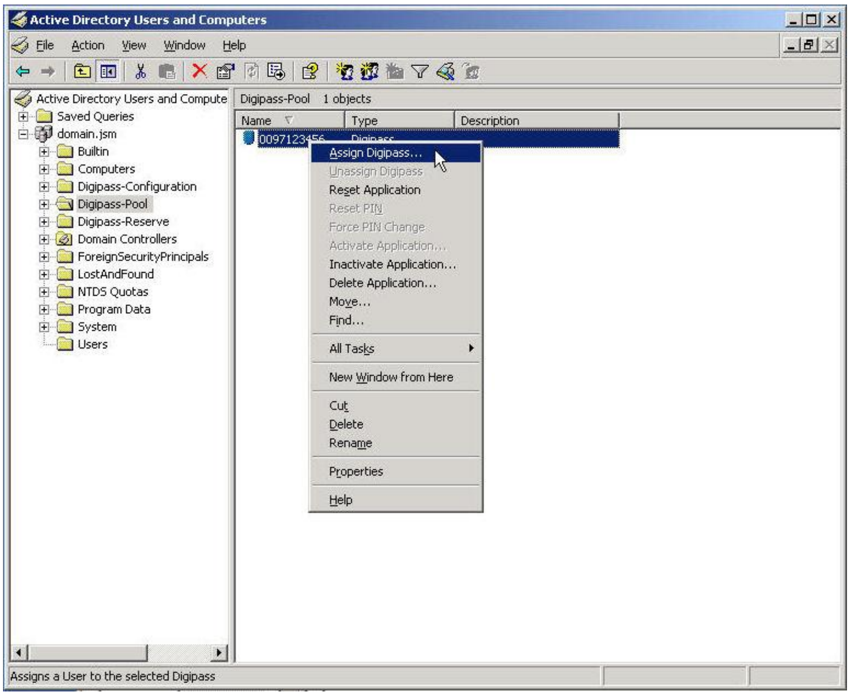


Name	Type	Description
testuser	User	
Telnet(		Members of this group ha...
SUPPO		This is a vendor's account ...
Schema		Designated administrators...
RAS ar		Servers in this group can ...
krbtgt		Key Distribution Center Se...
IWAM_		Built-in account for Intern...
IUSR_E		Built-in account for anony...
IIS_WF		IIS Worker Process Group
HelpSe		Group for the Help and Su...
Guest		Built-in account for guest ...
Group I		Members in this group can...
Enterpr		Designated administrators...
dppost		PostgreSQL service account
Domair		All domain users
Domair		All domain guests
Domair		All domain controllers in th...
Domair		All workstations and serve...
Domain Admins	Security Group ...	Designated administrators...
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
DnsAdmins	Security Group ...	DNS Administrators Group
citrix1	User	
Cert Publishers	Security Group ...	Members of this group are...
Administrator	User	Built-in account for admini...

Assigns a Digipass to the selected Users

Figure 34: DIGIPASS Assignment (1)

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

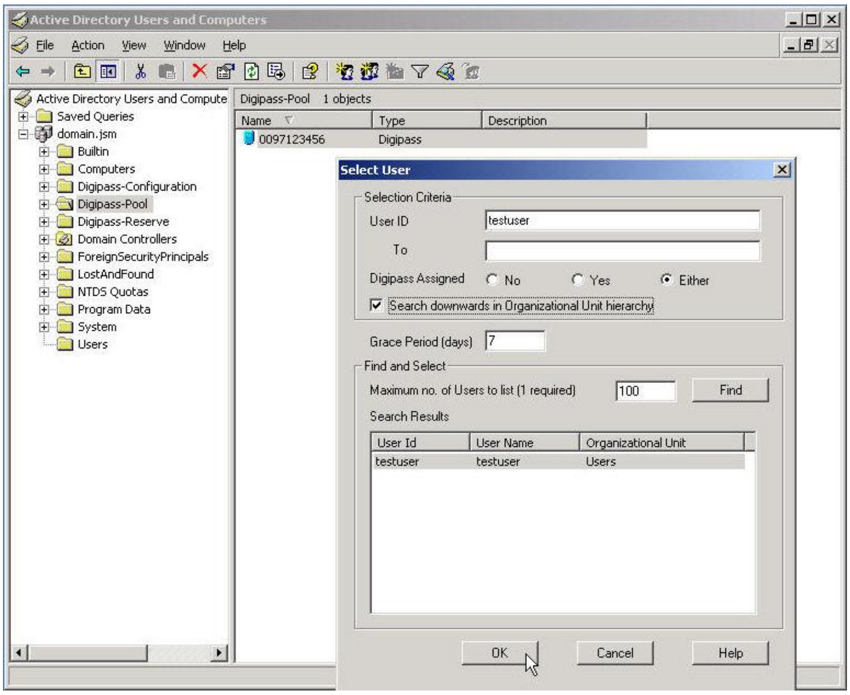


Name	Type	Description
0097123456	Digipass	

Assigns a User to the selected Digipass

Figure 35: 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.



Name	Type	Description
0097123456	Digipass	

Selection Criteria

User ID: testuser

To:

Digipass Assigned ○ No ○ Yes ● Either

☑ Search downwards in Organizational Unit hierarchy

Grace Period (days): 7

Find and Select

Maximum no. of Users to list (1 required): 100

Find

Search Results

User Id	User Name	Organizational Unit
testuser	testuser	Users

Figure 36: 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.

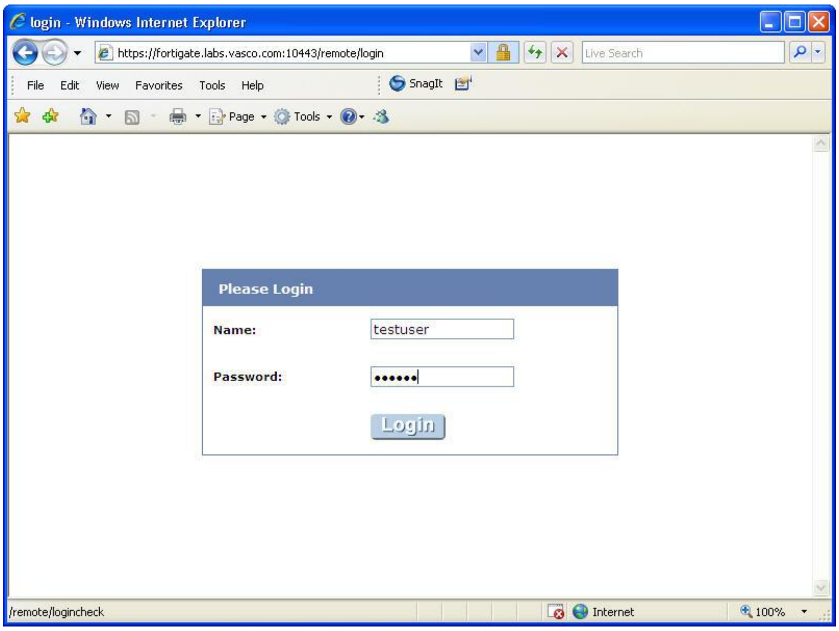
8 Fortigate SSL/VPN test

By default the Fortigate configures the SSL/VPN service on port 10443.

8.1 Response Only

To start the test, browse to the public IP address or hostname of the Fortigate device.

In our example this is https://fortigate.labs.vasco.com:10443. Enter your **Name** and **Password** (One Time Password) and click the **Login** button.


login - Windows Internet Explorer
https://fortigate.labs.vasco.com:10443/remote/login
Live Search
File Edit View Favorites Tools Help
SnagIt
Page Tools
Internet
100%

Please Login

Name: testuser

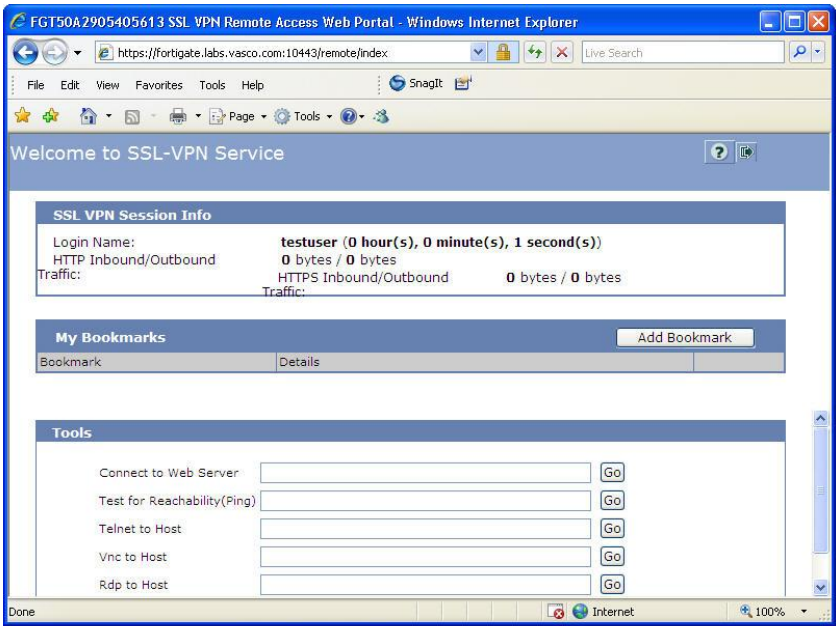
Password: ••••••

Login

/remote/logincheck

Figure 37: Response Only (1)

If all goes well, you will be authenticated and see the SSL/VPN portal page.


FGT50A2905405613 SSL VPN Remote Access Web Portal - Windows Internet Explorer
https://fortigate.labs.vasco.com:10443/remote/index
Live Search
File Edit View Favorites Tools Help
SnagIt
Page Tools
Done
Internet
100%

Welcome to SSL-VPN Service

SSL VPN Session Info

Login Name: testuser (0 hour(s), 0 minute(s), 1 second(s))

HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes

HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

My Bookmarks

Add Bookmark

Bookmark	Details

Tools

Connect to Web Server Go

Test for Reachability(Ping) Go

Telnet to Host Go

Vnc to Host Go

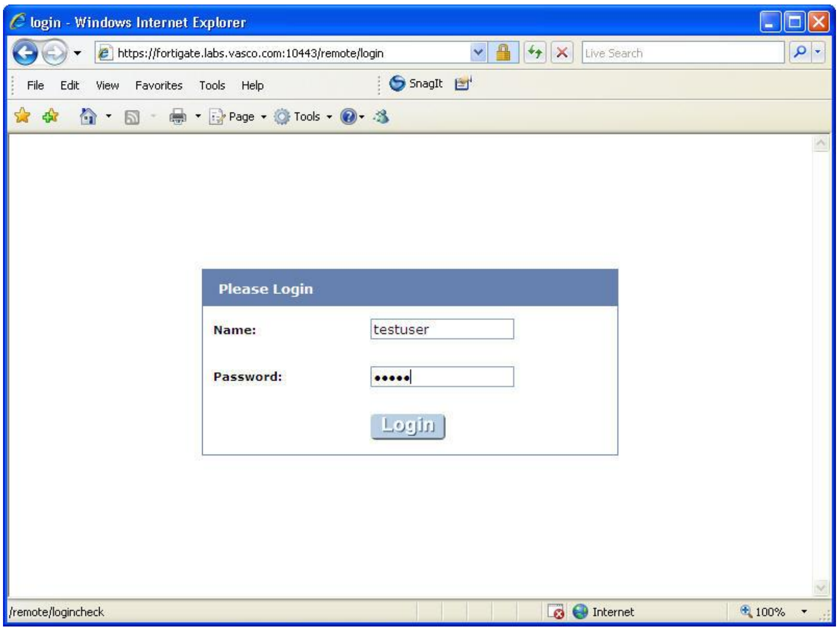
Rdp to Host Go

Figure 38: Response Only (2)

8.2 Challenge / Response

For the challenge response test, enter your **Name** and **Password** (challenge/response trigger). Click the Login button.

In our case the challenge/response trigger is the user's static password.



login - Windows Internet Explorer
https://fortigate.labs.vasco.com:10443/remote/login
Live Search
File Edit View Favorites Tools Help
SnagIt
Page Tools
/remote/logincheck
Internet
100%

Please Login

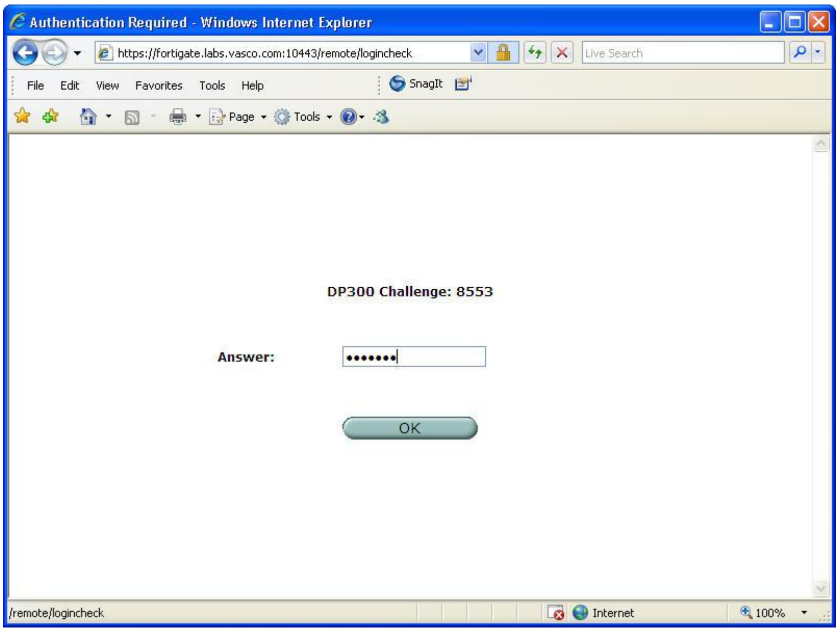
Name: testuser

Password: •••••

Login

Figure 39: Challenge / Response (1)

You will be presented with a **DP300 Challenge** code. Enter the **response** in the **Answer** field and click **OK**.



Authentication Required - Windows Internet Explorer
https://fortigate.labs.vasco.com:10443/remote/logincheck
Live Search
File Edit View Favorites Tools Help
SnagIt
Page Tools
/remote/logincheck
Internet
100%

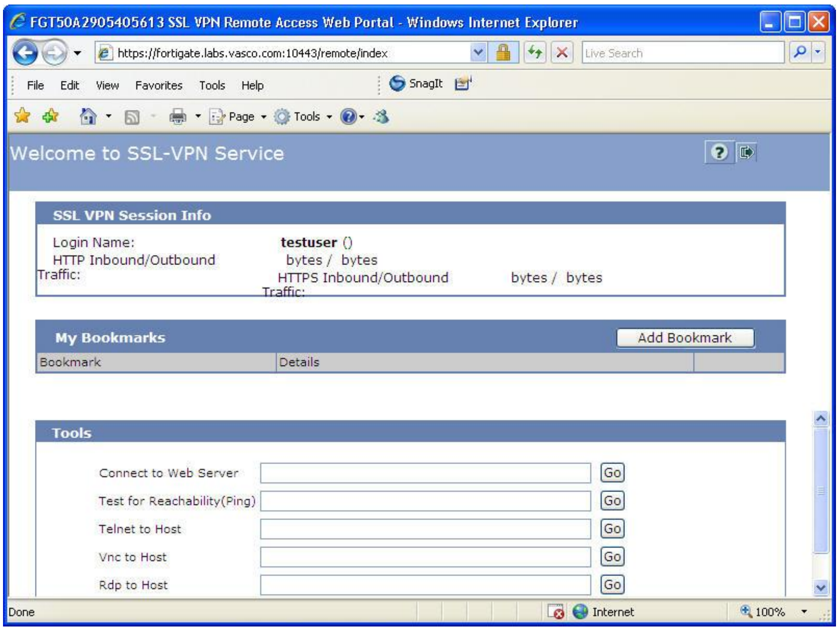
DP300 Challenge: 8553

Answer: •••••••

OK

Figure 40: Challenge / Response (2)

And if everything goes well, you will be shown the SSL/VPN portal page.



FGT50A2905405613 SSL VPN Remote Access Web Portal - Windows Internet Explorer
https://fortigate.labs.vasco.com:10443/remote/index
Live Search
File Edit View Favorites Tools Help
SnagIt
Page Tools
Done
Internet
100%

Welcome to SSL-VPN Service

SSL VPN Session Info

Login Name: testuser ()
HTTP Inbound/Outbound Traffic: bytes / bytes
HTTPS Inbound/Outbound Traffic: bytes / bytes

My Bookmarks

Add Bookmark

Bookmark	Details	

Tools

Connect to Web Server Go
Test for Reachability(Ping) Go
Telnet to Host Go
Vnc to Host Go
Rdp to Host Go

Figure 41: Challenge / Response (3)

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.

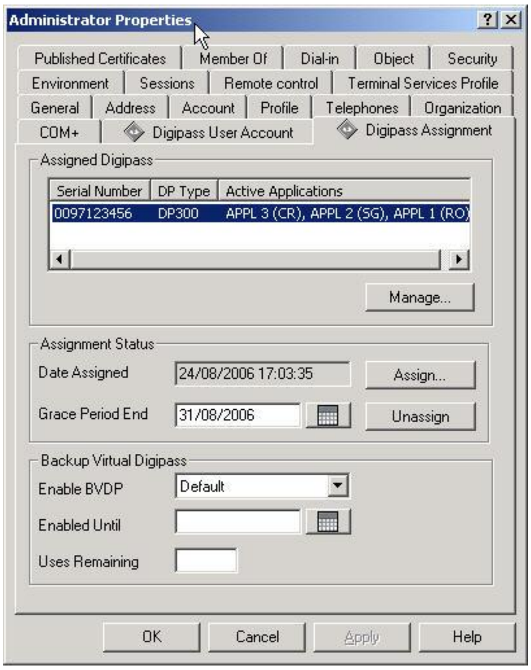
Backup Virtual DIGIPASS

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.



Assigned Digipass

Serial Number	DP Type	Active Applications
0097123456	DP300	APPL 3 (CR), APPL 2 (SG), APPL 1 (RO)

Assignment Status

Date Assigned: 24/08/2006 17:03:35

Grace Period End: 31/08/2006

Backup Virtual Digipass

Enable BVDP: Default

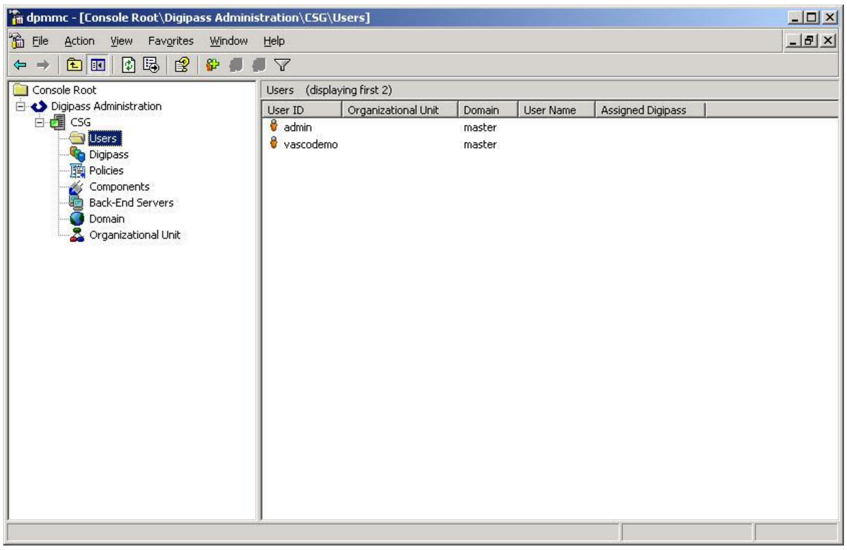
Enabled Until:

Uses Remaining:

Figure 42: 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 Administration\CSG\Users]

- Console Root
  - Digipass Administration
    - CSG
      - Users
      - Digipass
      - Policies
      - Components
      - Back-End Servers
      - Domain
      - Organizational Unit

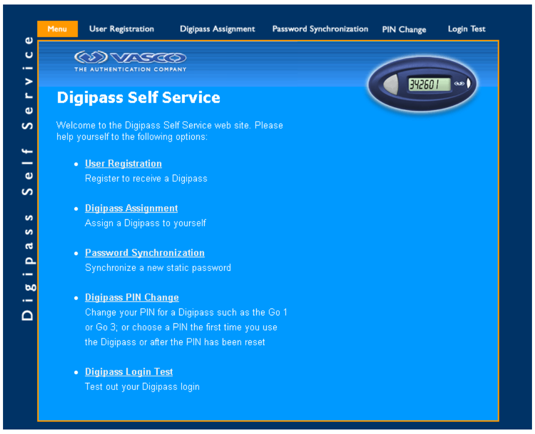
Users (displaying first 2)

User ID	Organizational Unit	Domain	User Name	Assigned Digipass
admin		master		
vascodemo		master		

Figure 43: 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.



Digipass Self Service

Welcome to the Digipass Self Service web site. Please help yourself to the following options:

- User Registration
  Register to receive a Digipass
- Digipass Assignment
  Assign a Digipass to yourself
- Password Synchronization
  Synchronize a new static password
- Digipass PIN Change
  Change your PIN for a Digipass such as the Go 1 or Go 3; or choose a PIN the first time you use the Digipass or after the PIN has been reset
- Digipass Login Test
  Test out your Digipass login

Figure 44: VM Features (3)

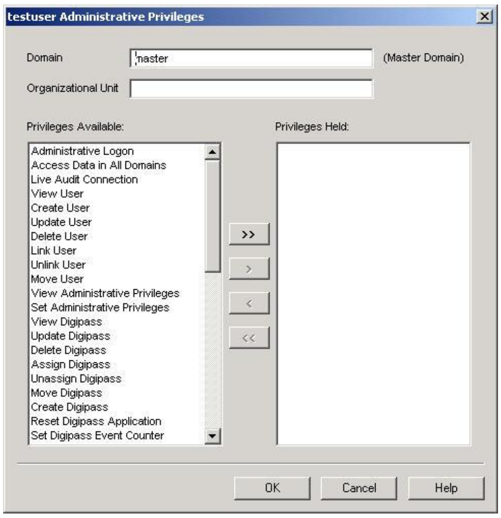
9.3.4 Delegated administration

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: master (Master Domain)

Organizational Unit:

Privileges Available:

Administrative Logon
Access Data in All Domains
Live Audit Connection
View User
Create User
Update User
Delete User
Link User
Unlink User
Move User
View Administrative Privileges
Set Administrative Privileges
View Digipass
Update Digipass
Delete Digipass
Assign Digipass
Unassign Digipass
Move Digipass
Create Digipass
Reset Digipass Application
Set Digipass Event Counter

Privileges Held:

Figure 45: 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.