

Digipass Authentication for the NETASQ IPS-Firewall

Table of Contents

1	Overview.....	3
2	Problem Description	3
3	Solution.....	3
4	Technical Concept General Overview	4
5	Configuration of the IPS-Firewall	5
5.1	Add VACMAN Middleware as a host.....	5
5.2	Enable RADIUS authentication.....	6
5.3	LDAP initialisation	9
5.4	Add a user in the internal LDAP database	13
6	Configuration of VACMAN Middleware.....	17
6.1	Set time and date.....	17
6.2	Configure VACMAN Middleware	18
6.3	Configure RADIUS Client	19
6.4	Import Demo DIGIPASS token secret	20
6.5	Create a Demo user.....	22
6.6	Assign Demo DIGIPASS token to demo user	23
6.7	Changing PINs.....	26
6.8	Test VACMAN Middleware with VASCO RADIUS Client Simulator.....	27
7	Logon example	30
8	VACMAN Middleware features	32
8.1	Installation.....	32
8.2	Deployment.....	32
8.3	Administration	34
8.4	Advanced Features.....	34
9	Conclusion.....	35
10	For more information on NETASQ.....	35
11	For more information on VASCO.....	35
12	About NETASQ	35
13	About VASCO Data Security	36

1 Overview

The purpose of this document is to show how the NETASQ IPS-Firewall can use VASCO's strong user authentication.

2 Problem Description

Today's business is built around information applications. To ensure business workflow, productivity and enhancing client relationships, internal network resources are increasingly being made accessible from anywhere.

The weakest link in any security infrastructure is the use of static passwords. These passwords are easily stolen, guessed, reused or shared. There is a need for strong user authentication, based on 2-factors: something you have and something you know.

3 Solution

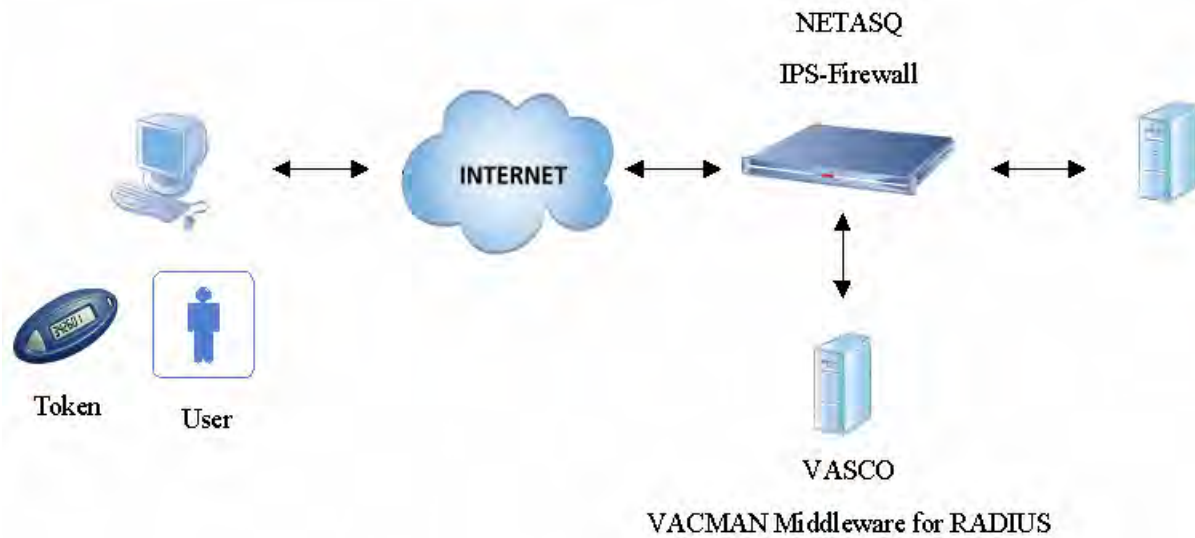
NETASQ's IPS-Firewalls address the key network security needs of small, mid-size and large departmental sites, service providers and remote users by providing cutting-edge technology on a complete product range. NETASQ's purpose-built security appliances all provide a multi-layered security approach that stops network and content-based threats at the edge of the network without compromising performance or requiring additional hardware.

In addition, every NETASQ IPS-Firewall includes real-time intrusion prevention, stateful firewall, content filtering, embedded KASPERSKY antivirus, Virtual Private Networking (VPN) and traffic shaping functionality in one easy to deploy, maintain and update security appliance.

VASCO's DIGIPASS enables users to generate One-Time Passwords that safeguard access to e-business and e-banking applications, to corporate networks and allow for more secure transactions. By using DIGIPASS patented technology, you eliminate the weakest link in any security infrastructure; the use of static passwords that are easily stolen, guessed, reused, or shared. It can be deployed as a small hand-held device, as a smart card reader, as software for computers, laptops, PDA's or cell phones.

4 Technical Concept General Overview

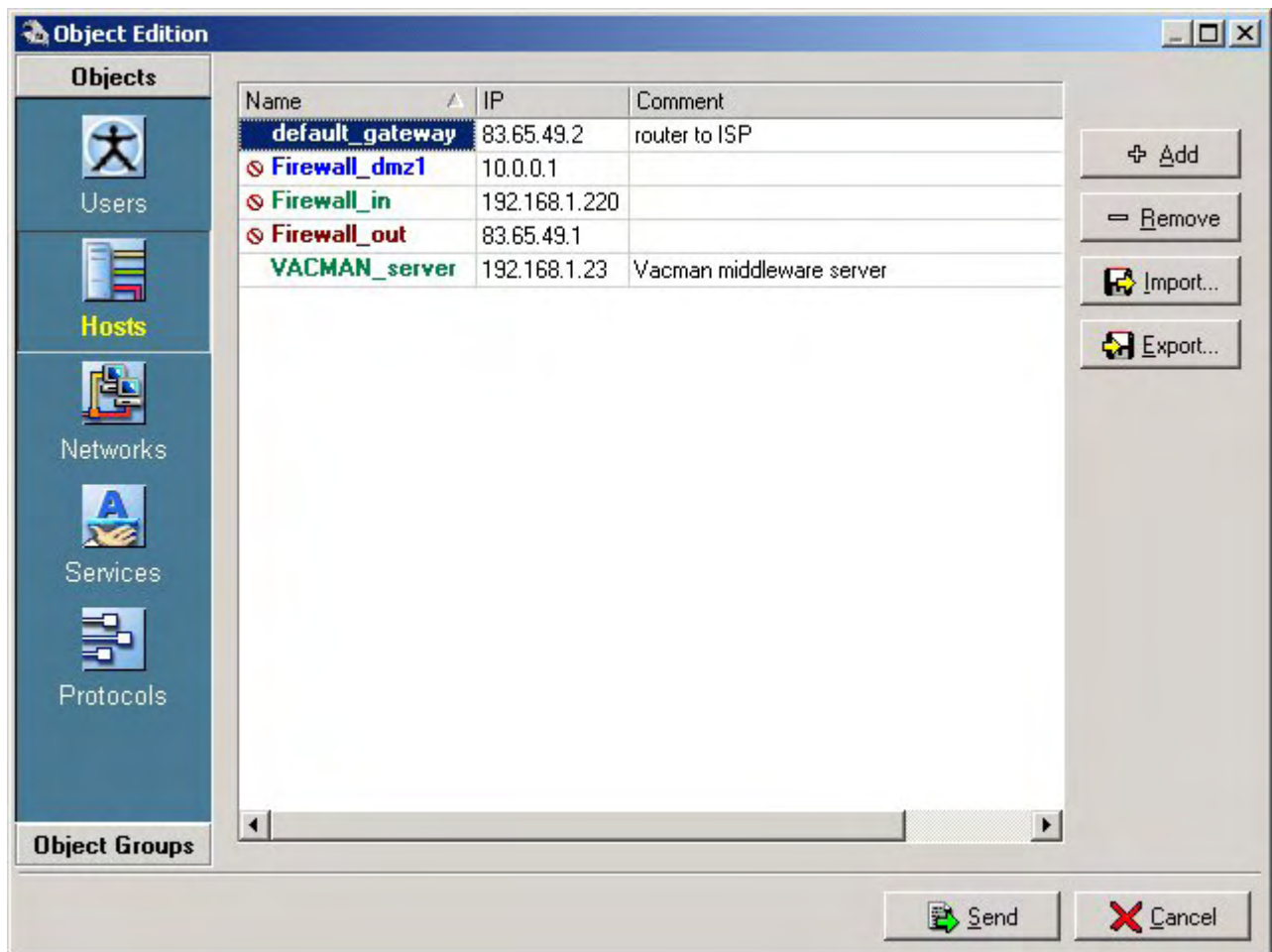
NETASQ IPS-Firewalls are purpose-built network security appliances that combine Firewall, Virtual Private Networking (VPN), Content Filtering and Real-Time Intrusion Prevention functionalities. Based on NETASQ's revolutionary "ASQ" in-line Intrusion Prevention Technology, all NETASQ IPS-Firewalls ensure the highest level of security.



By using the VASCO DIGIPASS, access to resources is not left to the mercy of an insecure password. Before granting a user access to a resource, the NETASQ IPS-Firewall will verify the token password with VASCO's VACMAN Middleware for RADIUS.

5 Configuration of the IPS-Firewall

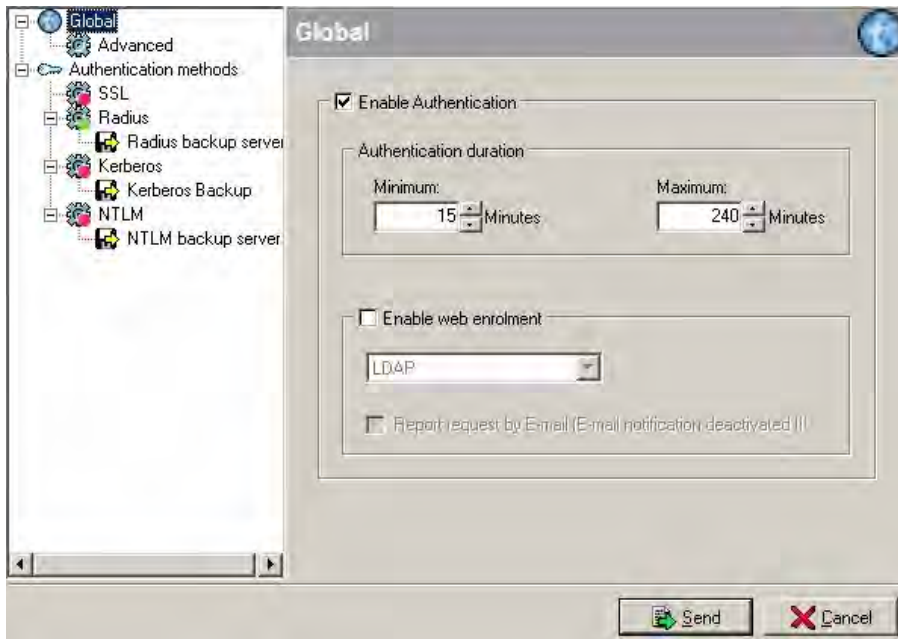
5.1 Add VACMAN Middleware as a host



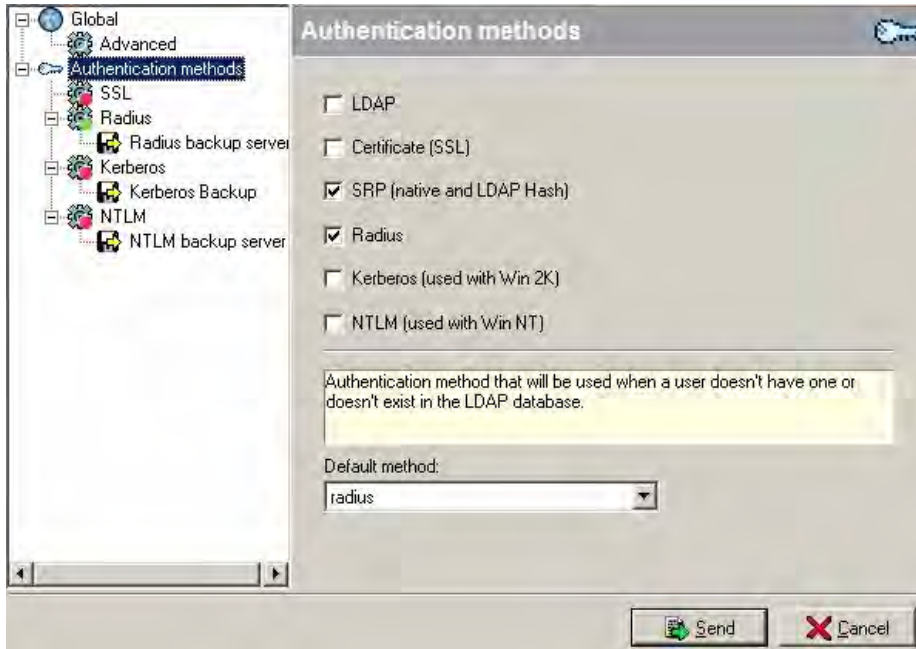
First of all the VACMAN Middleware for RADIUS needs to be added as a host on the IPS-Firewall. On the appropriate screen click on Add, specify a Name, an IP address and if desired a Comment. In this document the assumption is made that the VACMAN Middleware runs on IP address 192.168.1.23 and that 192.168.1.220 is the IP address of the internal interface of the IPS-Firewall.

5.2 Enable RADIUS authentication

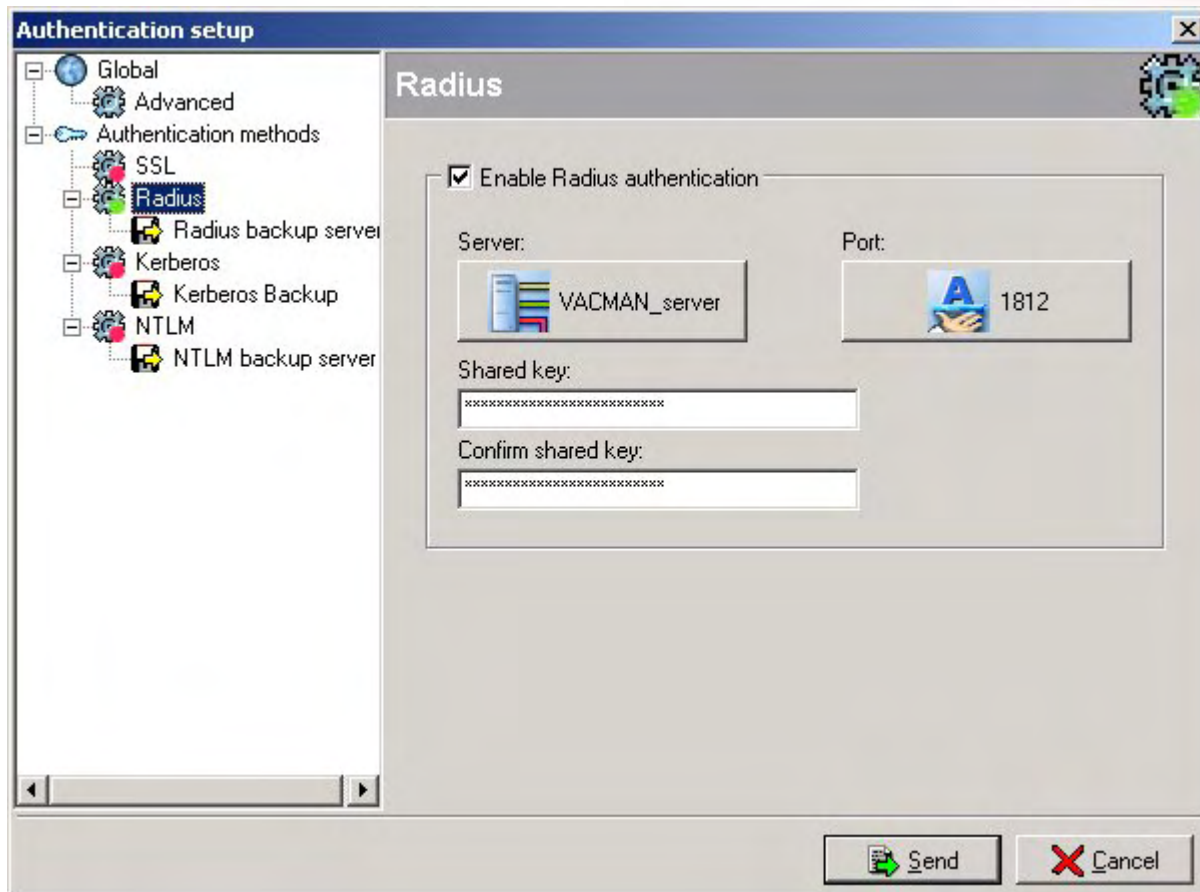
Go to authentication/global setup in the menu in the firewall manager. The following screen appears.



Enable Authentication needs to be checked. The minimum and maximum authentication period can be specified here. If both are the same, the end user will be able to specify the period himself.



On the Authentication methods screen, Radius needs to be checked. The icon next to Radius on the left part of the screen will turn green. Multiple authentication methods can be checked at once, allowing you to choose which user needs to use which method. Make sure to set the default method to Radius. This will make the firewall always go check the Radius database if a username does not exist in a local LDAP database on the firewall, or if an authentication method is not specified for that user.



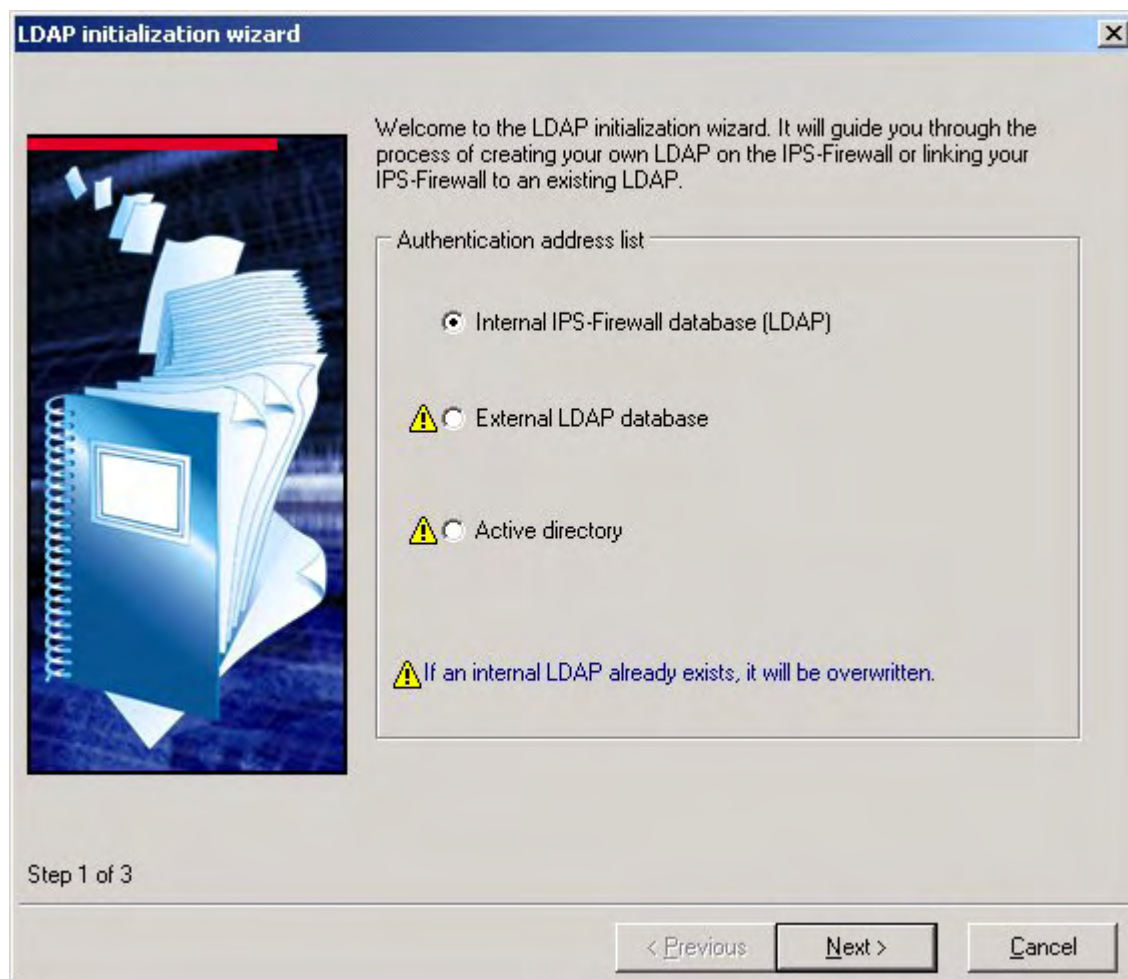
On the Radius screen, Enable Radius authentication needs to be checked. The Vacman middleware server needs to be selected by clicking on the Server button. The Port to be used for the authentication needs to be selected. The standard port is UDP 1812. If UDP 1645 needs to be used for RADIUS authentication on the IPS-Firewall, then you need to add this UDP port as an object (configuration/objects/services) first before it can be selected here. We will assume during the course of this document that UDP port 1645 is used by the VACMAN Middleware and that it has been added and has been selected on the IPS-Firewall. The shared secret needs to be filled in and confirmed. In this document we use 'vasco' as shared secret.

This is all the necessary configuration that needs to be done in order to have the IPS firewall proxy all authentication requests to the VACMAN middleware, which will then in turn inform the IPS firewall whether the authentication has been successful or not. If a more granular approach is required, like for instance if you want specific users to have different privileges in the filtering rules (for example an administrator needs to have access to more resources than a normal user), then you can also add these users in an internal LDAP database on the firewall. The drawback is that these objects need to be created manually; they cannot be imported from the radius database. A second requirement is that they need to have the same username in the internal LDAP database on the IPS firewall as in the external RADIUS database.

The way this needs to be configured is described below.

5.3 LDAP initialisation

In the firewall manager, go to authentication/LDAP database. The LDAP initialisation wizard starts & following screen appears.



Choose internal LDAP database and click next.

Fill in the necessary fields according to your specific location & company.

LDAP initialization wizard

Internal IPS-Firewall LDAP database

Organisation name (o):
company-name

Domain country (dc):
belgium

LDAP administration password: (minimum 8 characters)

Confirm LDAP administration password:

Public LDAP configuration

Set public LDAP

Activate plaintext access

Activate SSL access

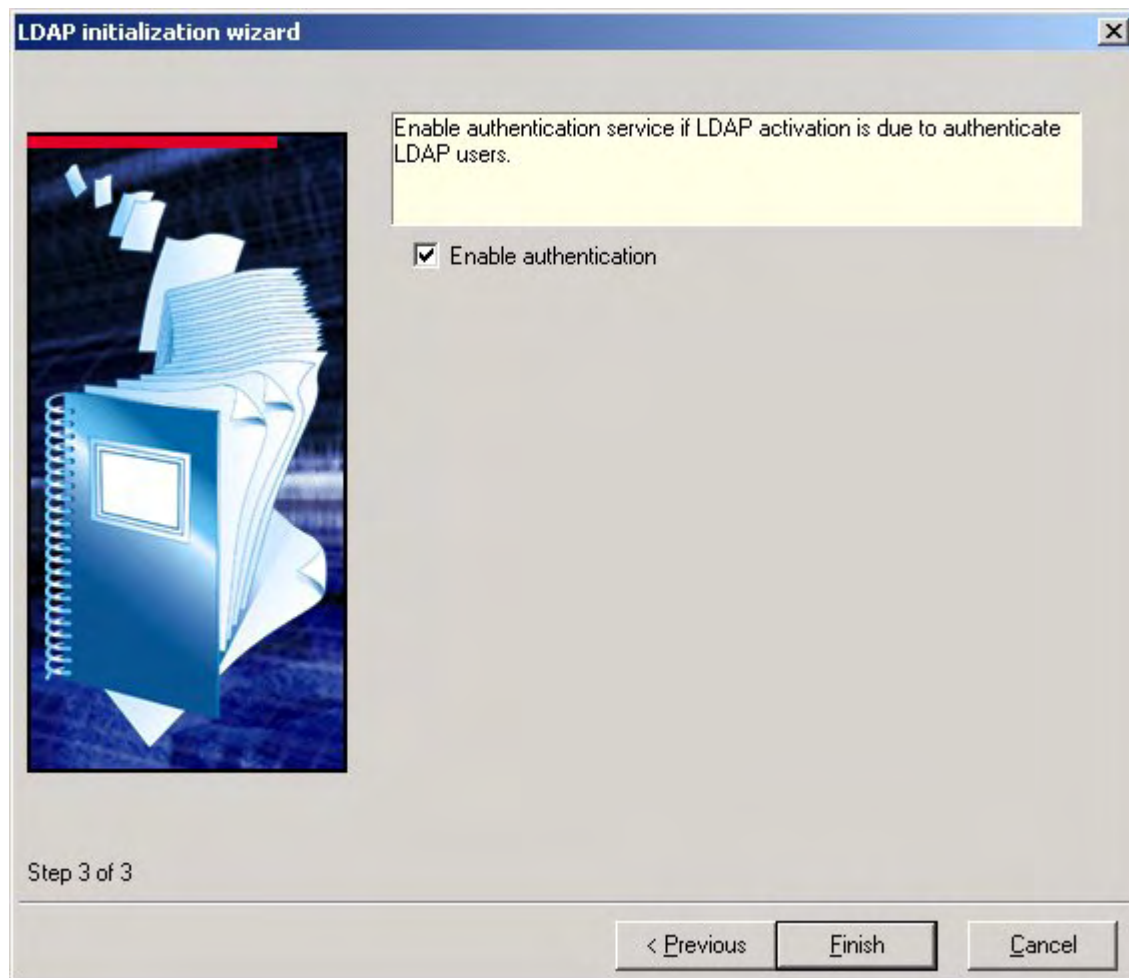
<Choose a certificate>

Step 2 of 3

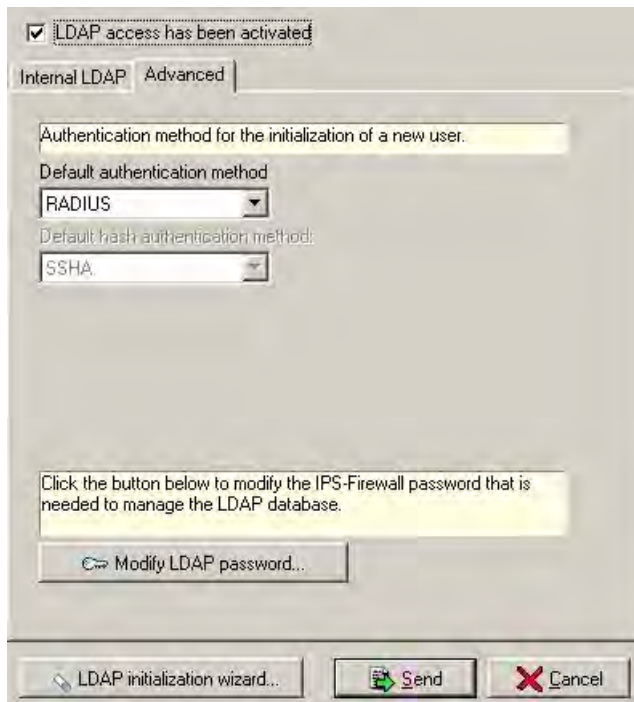
< Previous Next > Cancel

Click next.

Leave the checkbox 'enable authentication' marked and click finish. An internal LDAP database will be created, a process that takes a while on the smaller models like an F50.



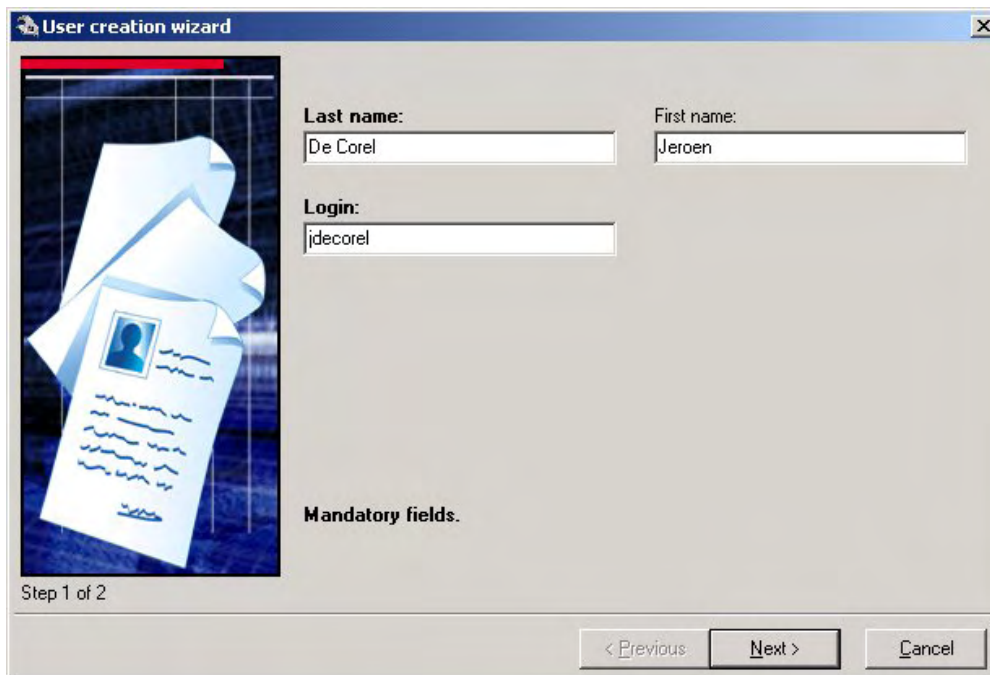
Now the following screen appears, allowing you to change the LDAP database properties.



Go to the Advanced tab page to select RADIUS as Default authentication method. This will make sure A user can be added to the IPS-Firewall and Radius authentication can be enabled for that user. We already configured the IPS-Firewall to use Radius authentication for unknown users as well (cf. page 6 of this document; default authentication method)

5.4 Add a user in the internal LDAP database

Now we can add a user in the internal LDAP database. Go to configuration/objects/users and click "add".



User creation wizard

Last name: De Corel

First name: Jeroen

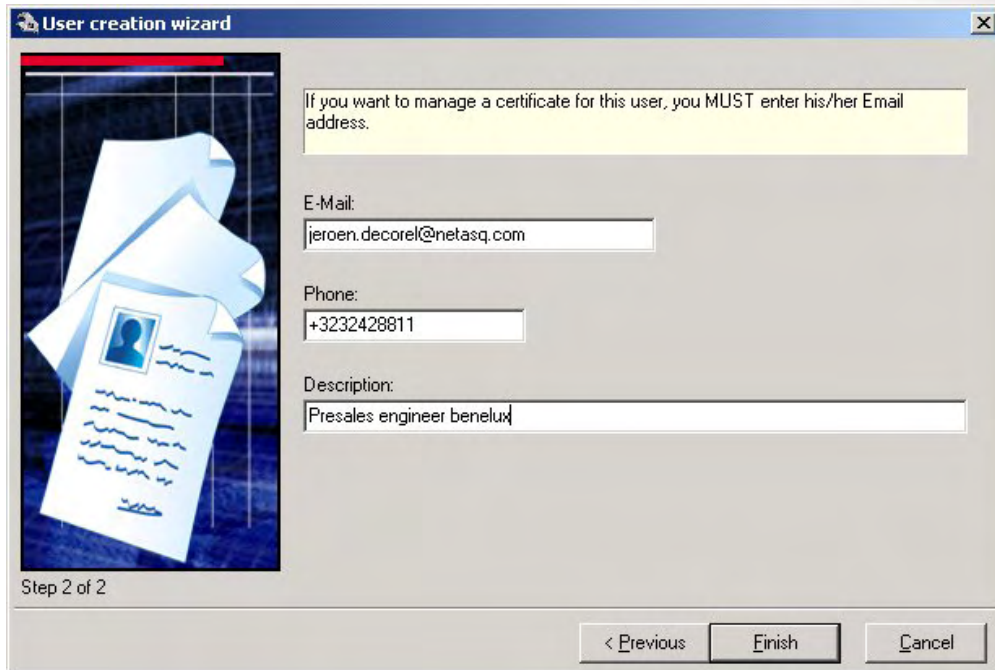
Login: jdecorel

Mandatory fields.

Step 1 of 2

< Previous Next > Cancel

Fill in the necessary details and click next.



The image shows a Windows-style dialog box titled "User creation wizard". On the left side, there is a graphic of a stack of papers with a blue ID card on top. The main area of the dialog contains a yellow warning box at the top with the text: "If you want to manage a certificate for this user, you MUST enter his/her Email address." Below this are three input fields: "E-Mail:" with the value "jeroen.decorel@netasq.com", "Phone:" with the value "+3232428811", and "Description:" with the value "Presales engineer benelux". At the bottom left, it says "Step 2 of 2". At the bottom right, there are three buttons: "< Previous", "Finish", and "Cancel".

User creation wizard

If you want to manage a certificate for this user, you MUST enter his/her Email address.

E-Mail:
jeroen.decorel@netasq.com

Phone:
+3232428811

Description:
Presales engineer benelux

Step 2 of 2

< Previous Finish Cancel

Fill in the necessary details and click next.

User edition

User | Authentication | Privileges

Jeroen De Corel

Name : **First name :**

Login : **E-mail address:**

Phone :

Description :

Fill in the necessary details and click next.

User edition

User | Authentication | Privileges

Authentication

Allow authentication

SRP (LDAP hash)

SRP

LDAP

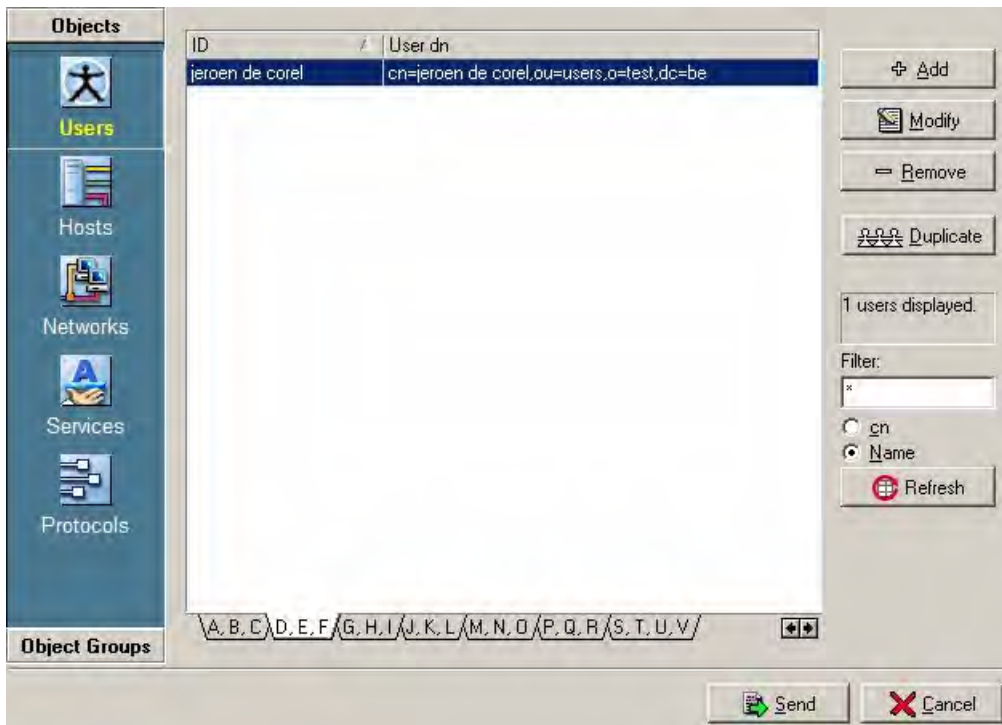
These methods do not use LDAP user's password

Certificate (SSL) NTLM

Radius Kerberos

Make sure to mark the "allow authentication" checkbox and choose Radius. Click Send.

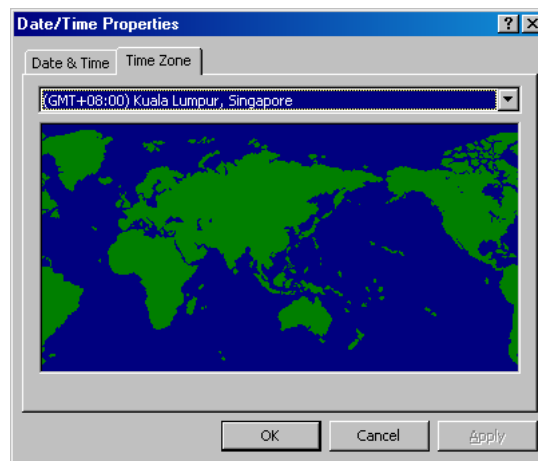
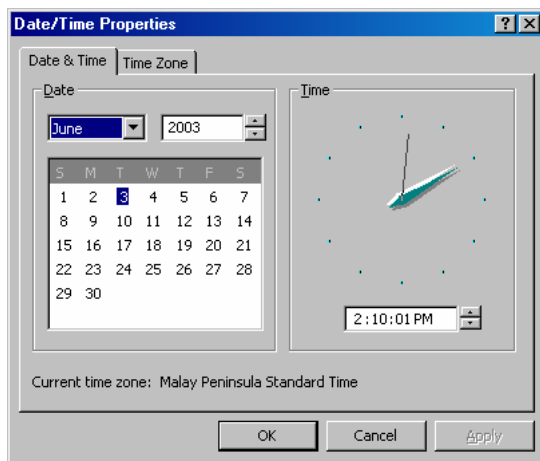
The user is now created in the LDAP database and the firewall will verify the password with the Radius database via the VACMAN middleware server. The user is now visible in the list if the appropriate tab is chosen at the bottom (pick the letter of the last name of the newly created user)



6 Configuration of VACMAN Middleware

6.1 Set time and date

The DIGIPASS token is based on Time Synchronization. All tokens are created with their internal real time clock set to GMT. As such, it is important to set the date, time and time zone of the server running the VACMAN Middleware correctly so that GMT can be derived correctly.



6.2 Configure VACMAN Middleware

Start the VACMAN Middleware and select the Admin Console. Configure the settings as shown below. The 'Server IP' refers to the IP address of the server running the VACMAN Middleware and thus it is set to 192.168.1.23.

Assuming that there is no third party RADIUS Server in this setup, and that the VACMAN Middleware is used to handle authentication only, you can then select the 'Authenticator' as 'Local Server'.

The RADIUS Client is using RADIUS ports for authentication and accounting and thus 'Incoming RADIUS Authentication Port' and 'Incoming RADIUS Accounting Port' should be set to 1645 (1812) and 1646 (1813) respectively.

To save the VACMAN Middleware setting, click on the 'Diskette' button or the 'File'->'Save' menu as shown.

The screenshot displays the VACMAN Middleware Admin GUI. The window title is "VACMAN Middleware - Admin GUI". The interface includes a menu bar (File, Look & Feel, Help) and a toolbar with icons for refresh, add, delete, save, and help. A left-hand navigation pane shows a tree structure under "VACMAN Middleware" with items: VM Server (192.168.1.23), RADIUS Client, RADIUS Proxy, User, and Token. The main content area has tabs for "Server", "RADIUS", "User", and "Token", with "Server" selected. The "Server Settings" section contains the following fields:

- Server IP: 192.168.1.23
- Worker Threads: 5
- Maximum Consoles: 3
- Admin TCP Port: 20003
- Replication Server IP: 0.0.0.0
- Incoming RADIUS Authentication Port: 1645
- Incoming RADIUS Accounting Port: 1646
- Authenticator: Proxy Server (dropdown menu is open, showing options: Local Server, Proxy Server, Local and Proxy, Windows, Local and Windows, Disabled)
- Cache use:
- Enable Del:

The "Auto Manage" and "Audit" tabs are visible. The "Automatic Management Options" section includes:

- Autoassign Token on User Create:
- Dynamic User Registration:
- Token Appl. Name: [dropdown]
- Password Autolearn:
- Grace Period (days): 7
- Stored Password Proxy:
- Email Server IP: [text box]
- Email Server Port: 25
- Email Alert List: [text box]

The "Update History" section shows:

- Created On: 06/15/2004 10:34:56 AM
- Last Modified On: 06/15/2004 11:36:49 AM

A status bar at the bottom of the window displays the message: "Request successfully processed."

6.3 Configure RADIUS Client

Select the RADIUS Client and configure the settings as shown below. Click on the 'New' button to enter the IP address and shared secret of a new RADIUS Client as shown. The 'IP Address' refers to that of the RADIUS Client used in the setup and thus it is set to 192.168.1.220. The 'Shared Secret' is set to 'vasco'. Note that the corresponding shared secret will have to be set at the RADIUS Server configuration within the IPS-Firewall. Click on the 'Save' button to save the configuration.

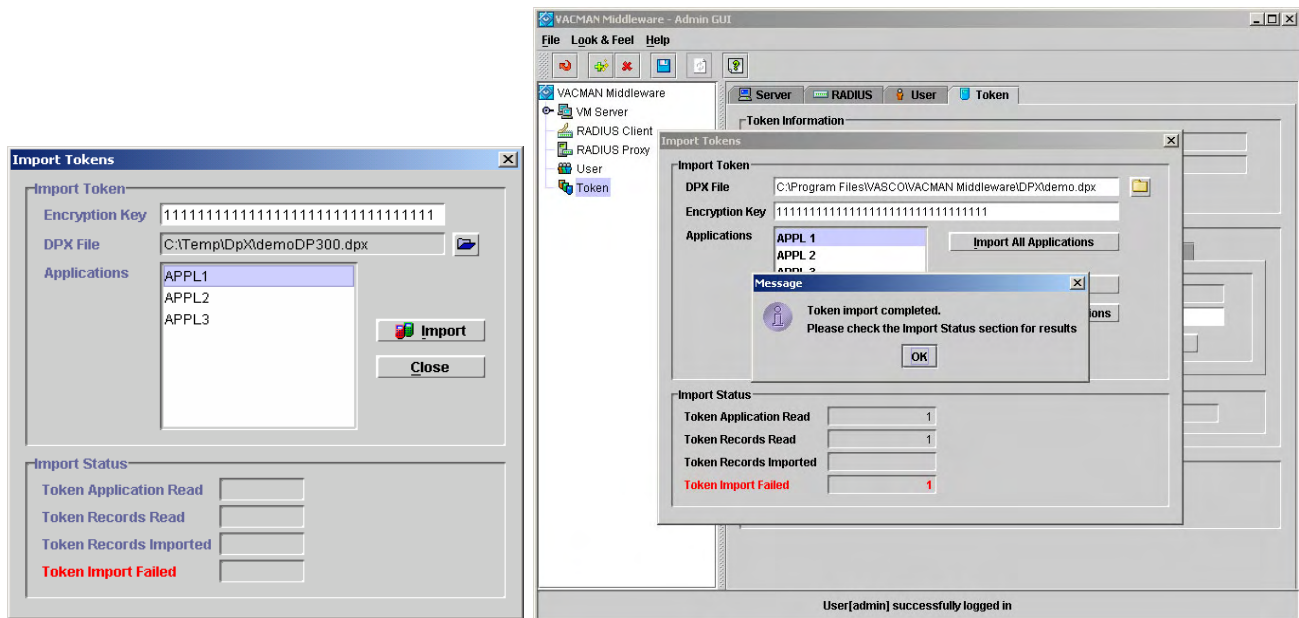
The screenshot displays the VACMAN Middleware Admin GUI. The window title is "VACMAN Middleware - Admin GUI". The menu bar includes "File", "Look & Feel", and "Help". The main interface has tabs for "Server", "RADIUS", "User", and "Token". Under the "RADIUS" tab, there are sub-tabs for "Client" and "Proxy". The "Client" sub-tab is active, showing the "RADIUS Client Settings" table. The table has three columns: "IP Address", "Shared Secret", and "Proxy". The first row is highlighted in blue and contains the values "192.168.1.220", "*****", and a checked checkbox. The second row contains "default", "*****", and a checked checkbox. To the right of the table are three buttons: "New", "Save", and "Delete". Below the table is an "Update History" section with two fields: "Created On" (06/15/2004 11:38:13 AM) and "Last Modified On" (06/15/2004 11:38:13 AM). At the bottom of the window, a status bar displays the message "Request successfully processed."

IP Address	Shared Secret	Proxy
192.168.1.220	*****	<input checked="" type="checkbox"/>
default	*****	<input checked="" type="checkbox"/>

The DPX file contains secret information relating to the token and thus it is encrypted. In order for VACMAN Middleware to decrypt such DPX file, you will have to enter the key. In order to decrypt a demo DPX file that contains secret information relating to a demo token, the encryption key is 32 digits of '1' as shown above.

Click on the Folder button to select the path for the DPX file. The name for a demo DPX file for a DIGIPASS Pro 300 token is typically 'demo.dpx' while the demo DPX file for a DIGIPASS GO 1 is typically 'demoGO1.dpx' and it can be found in the DPX subdirectory of the VACMAN Middleware installation directory.

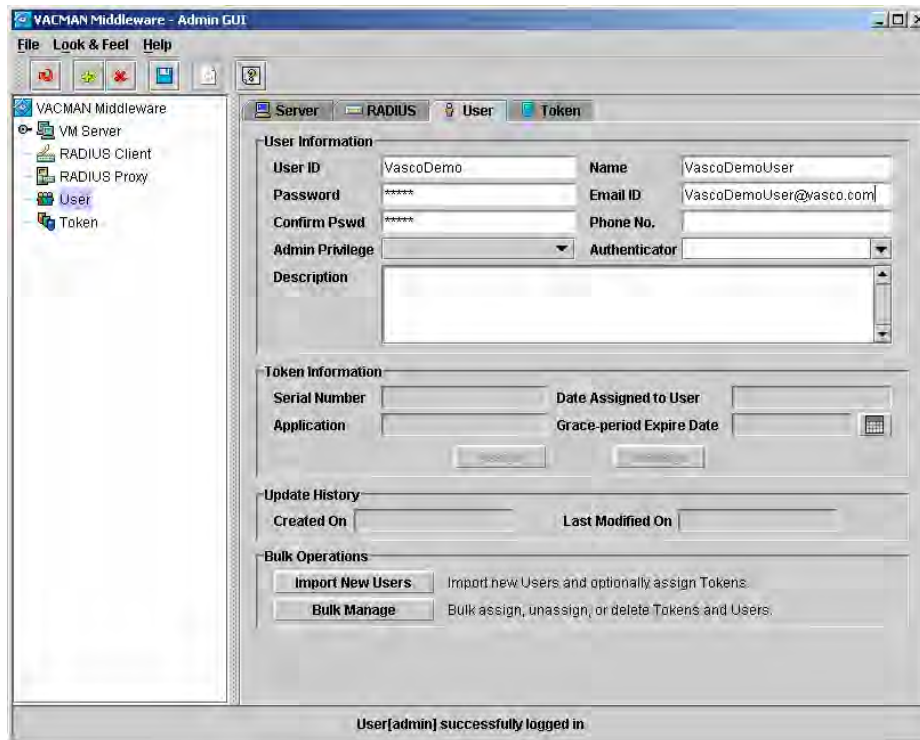
Select 'APPL 1' for one time password application of either the demo DIGIPASS Pro 300 token or DIGIPASS GO1 token and click the 'Import' button as shown.



Upon successful import, a message will be displayed, click on 'OK' button. Check the number of 'Token Application Read'. 'Token Records Read' and 'Token Records Imported' to ensure that 1 token has been successfully imported into the VACMAN Middleware. Click on the 'Close' button after finishing importing the token.

6.5 Create a Demo user

Select User and configure the following settings. Assuming that user 'VascoDemo' with password 'password' is to be created, click on the 'Diskette' button or the 'File'-'>'Save' menu to save the user.



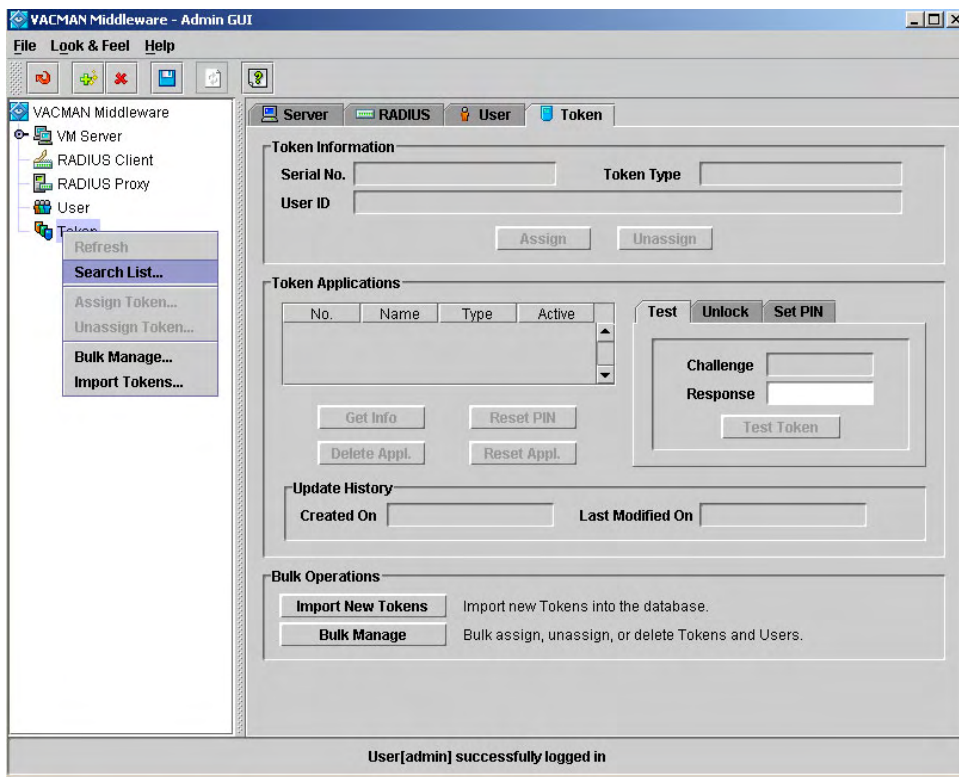
The screenshot shows the YACMAN Middleware Admin GUI. The window title is "YACMAN Middleware - Admin GUI". The menu bar includes "File", "Look & Feel", and "Help". The left sidebar shows a tree view with "YACMAN Middleware" expanded, containing "VM Server", "RADIUS Client", "RADIUS Proxy", "User", and "Token". The main content area has tabs for "Server", "RADIUS", "User", and "Token", with "User" selected. The "User" tab displays the following configuration fields:

- User Information:**
 - User ID: VascoDemo
 - Name: VascoDemoUser
 - Password: *****
 - Confirm Pswd: *****
 - Admin Privilege: (dropdown menu)
 - Authenticator: (dropdown menu)
 - Description: (text area)
 - Email ID: VascoDemoUser@vasco.com
 - Phone No.: (text field)
- Token Information:**
 - Serial Number: (text field)
 - Date Assigned to User: (text field)
 - Application: (text field)
 - Grace-period Expire Date: (calendar icon)
- Update History:**
 - Created On: (text field)
 - Last Modified On: (text field)
- Bulk Operations:**
 - Import New Users:** Import new Users and optionally assign Tokens.
 - Bulk Manage:** Bulk assign, unassign, or delete Tokens and Users.

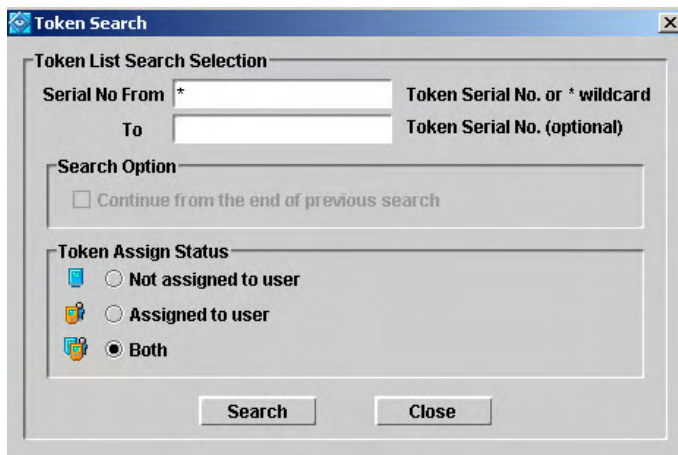
At the bottom of the window, a status bar displays the message: "User[admin] successfully logged in".

6.6 Assign Demo DIGIPASS token to demo user

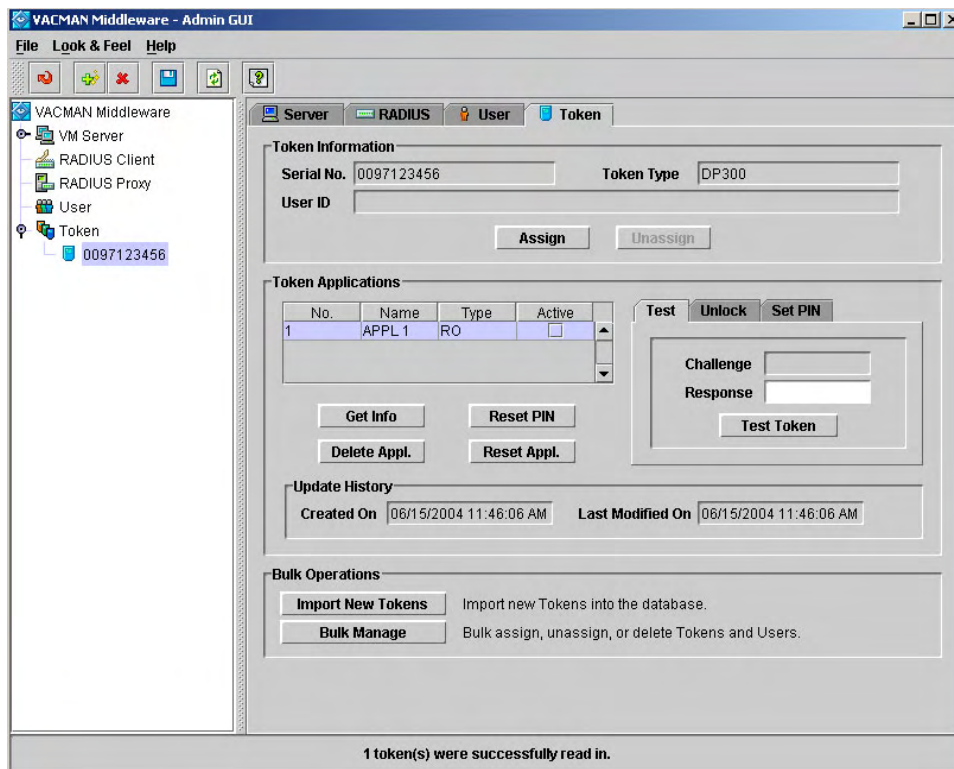
Right click on 'Token' and select 'Search List...' as shown.



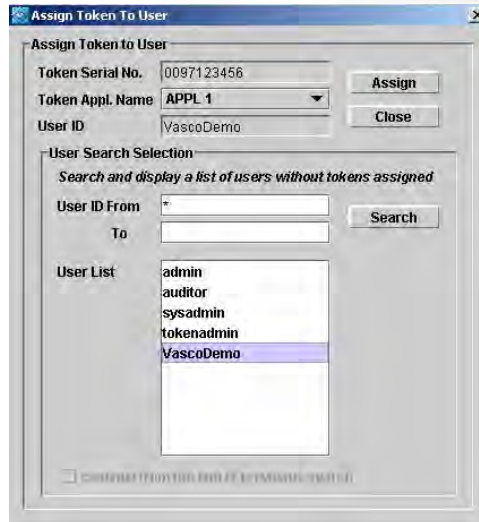
Select 'Both' to search for all tokens within the VACMAN Middleware and click on the 'Search' button.



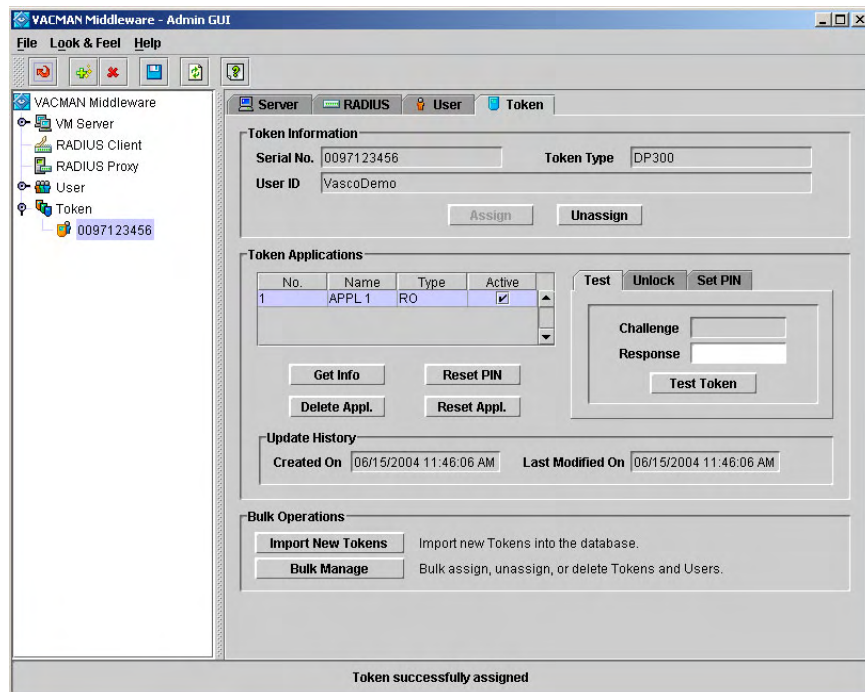
The serial number of the imported token should be displayed under Token as shown. The '0097123456' refers to the serial number of the demo token that is imported from the DPX file.



Click on the 'Assign' button to assign the token to a user. In order to search for all users available, click on the 'Search' button as shown below.



Select user 'VascoDemo', click on the 'Assign' button and see that demo token serial '0097123456' has been assigned to user 'VascoDemo'.



At this stage, the VACMAN Middleware has been successfully installed and configured to communicate with the IPS-Firewall at IP address 192.168.1.23 and the user 'VascoDemo' has been successfully created and assigned a demo DIGIPASS Pro 300 token.

6.7 Changing PINs

The DIGIPASS Pro series of tokens have a small keyboard so a PIN is changed on the physical token. With a DIGIPASS Go-1 and Go-3, a user's PIN is entered in the password field before the DIGIPASS code (eg. MyPIN896321). A Go-1 or Go-3's PIN can be alphanumeric (any combination of 0-9, A-Z and a-z) if desired. For simplicity it is still referred to as a PIN. A space cannot be used in the PIN. If you are using Go-1/3's and you decide to use the DIGIPASS record that has a PIN you obviously must allow the user and/or administrator to change the PIN. There are 2 methods to change the PIN. The users can change a PIN by entering the following in their logon page's password field.

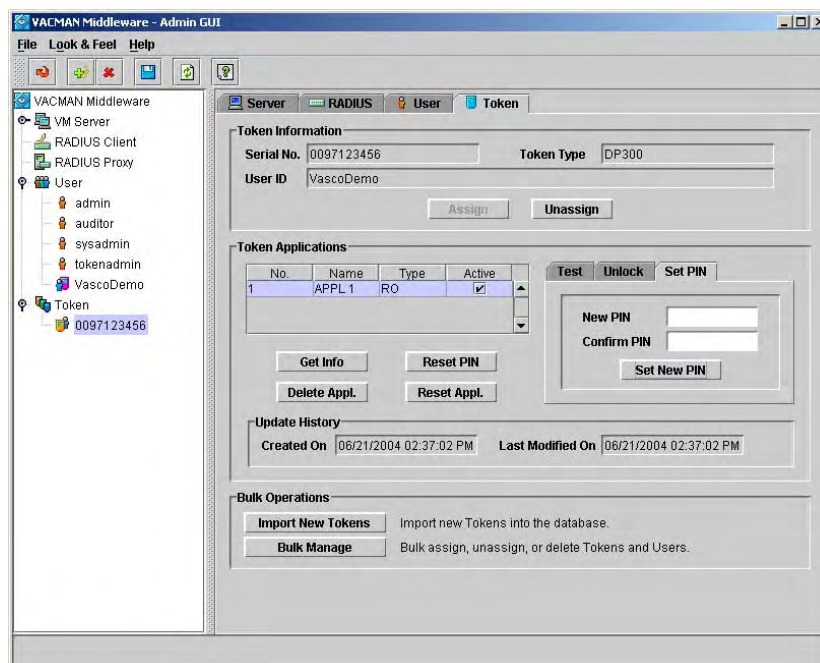
Password = Existing PIN + One Time Password + New PIN + New PIN

User Name

Password

Please note: If any of the supplied information is incorrect the PIN will not be updated. The new PIN must fit the PIN length parameters as when the DIGIPASS is programmed.

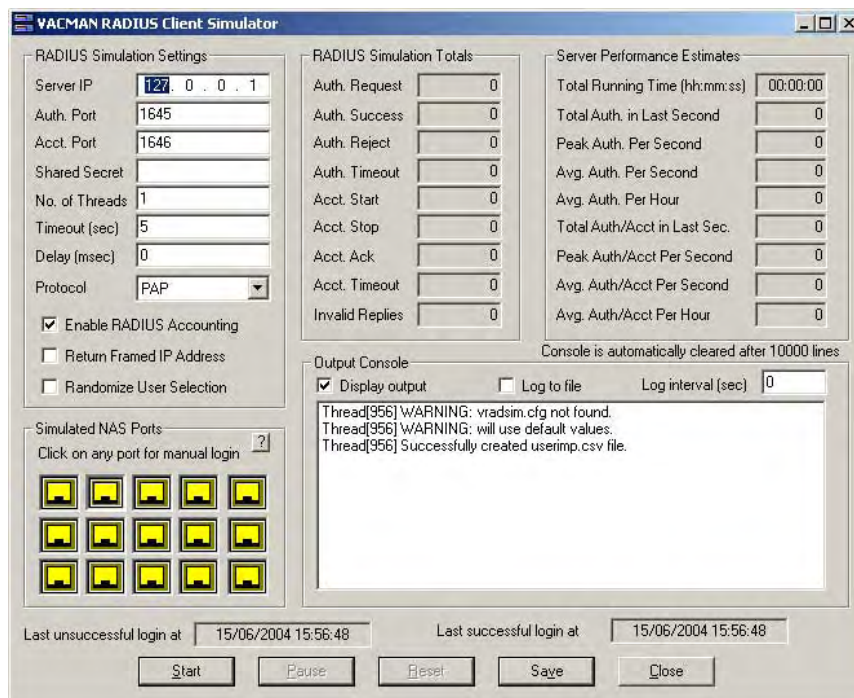
An administrator can change a PIN via the Administration Interface by going to the Token tab on the left hand side of the administration interface screen. On your right you click on Set PIN. There you write the New PIN and confirm it. Then you click on Set New PIN.



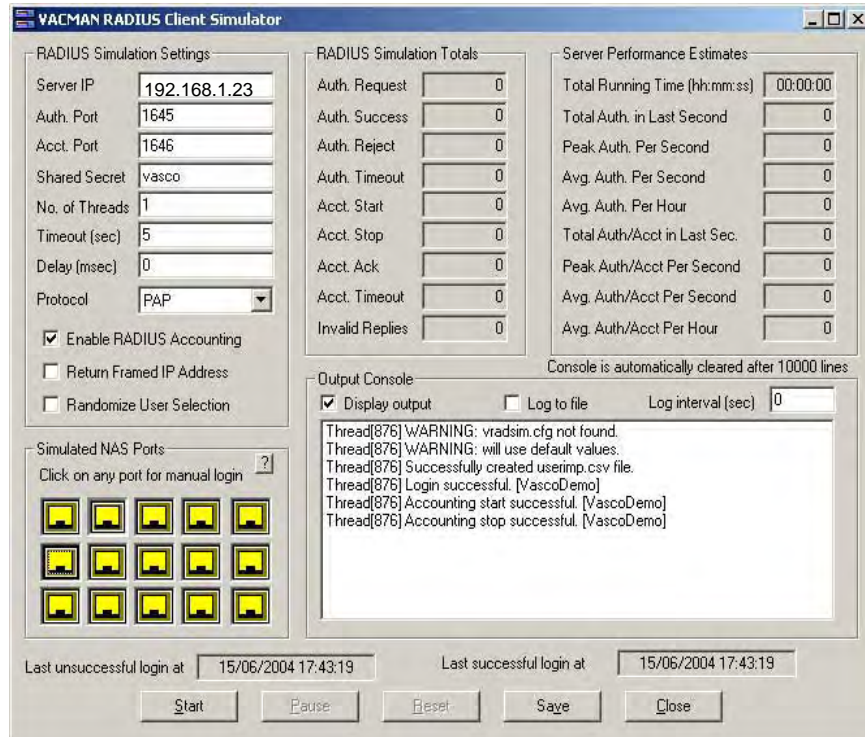
6.8 Test VACMAN Middleware with VASCO RADIUS Client Simulator

The VACMAN RADIUS Client Simulator (RCS) is a program that simulates RADIUS Authentication and Accounting processing in a similar fashion to RADIUS enabled NAS and Firewall devices. The RCS can be used to test user (and static-password) authentication, (DIGIPASS) token password authentication, estimate RADIUS server performance, system overload, and assist in detection of resource (memory, handle, etc.) leakage.

Install and open the Radius Client Simulator. When you open it you will see this:

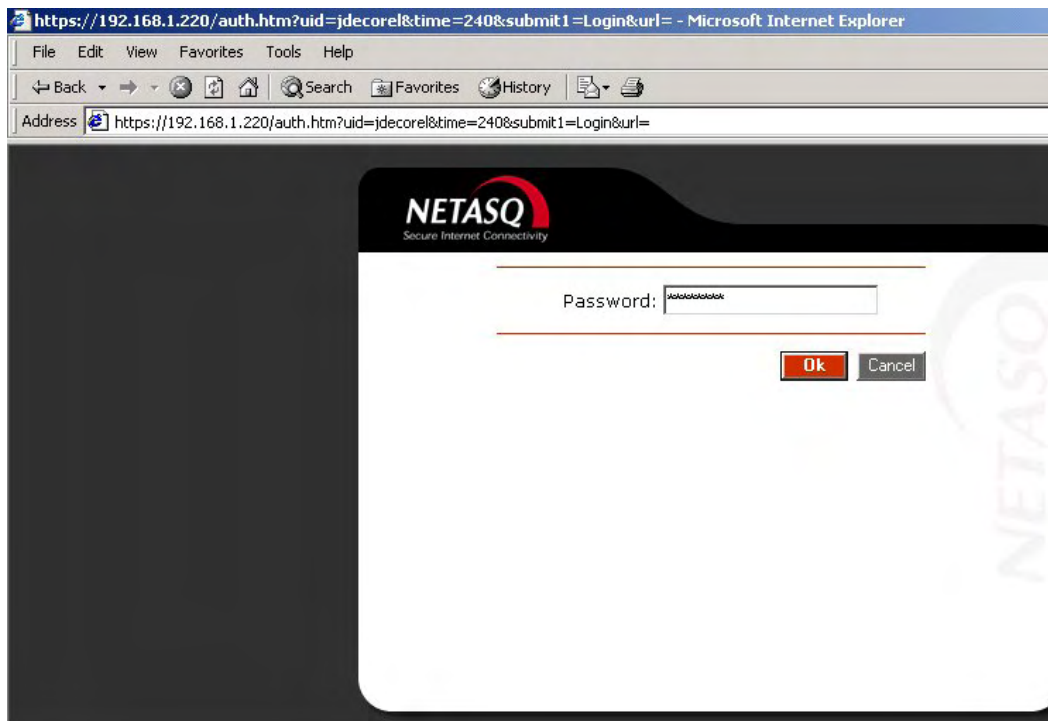
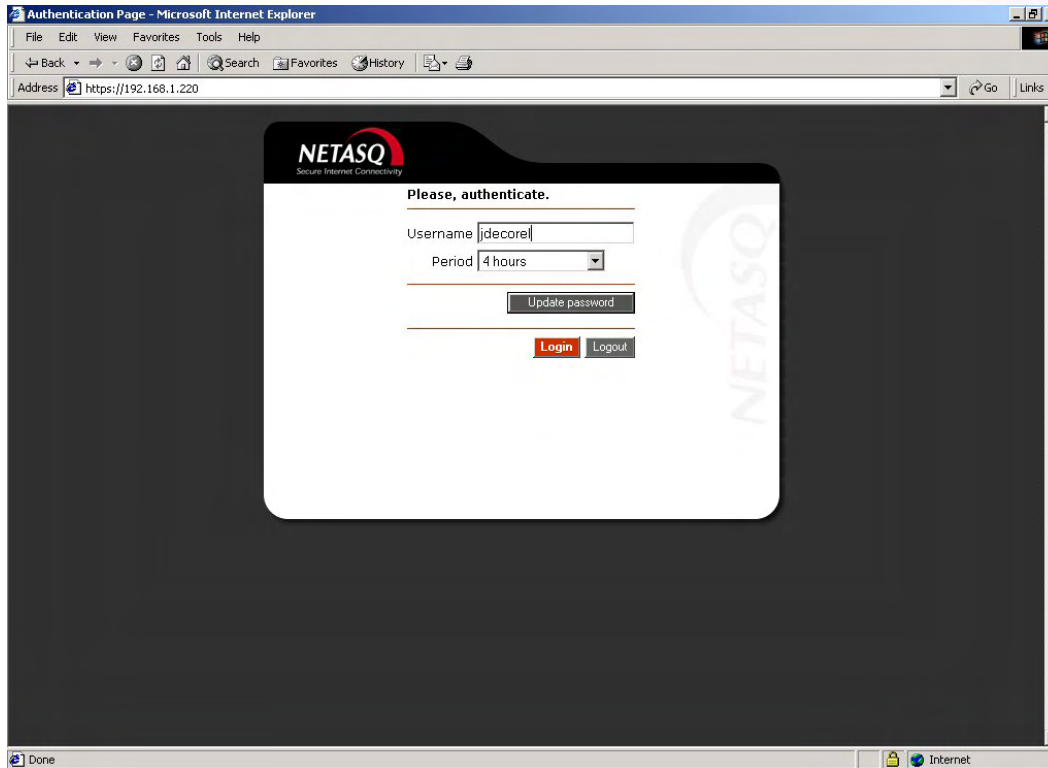


Then you fill in the Server IP and your Shared Secret. The RCS must be defined as a RADIUS client in the VACMAN Middleware.



Then you click one of the yellow ports, allowing you to enter User ID and password. In the User ID field you enter VascoDemo. (The test user we have created.) In the password field you enter the One Time Password (OTP) generated by the 1st application of the DIGIPASS. If you do not have a demo DIGIPASS you can get one by downloading from the VASCO website the DIGIPASS for Windows. This you can find here: <http://www.vasco.com/support/download.html?download=23>. Install it properly and run it. Go to Internet Banking. In "Authentication" you will find your password. As an alternative you can also go to <http://demotoken.vasco.com>.

7 Logon example






Authentication Success - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Back Forward Stop Home Search Favorites History

Address <https://192.168.1.220/plain.htm>



Authentication successful

You are logged in.



8 VACMAN Middleware features

8.1 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.

Support for Windows 2003 and IIS6

VM can be installed on Windows NT, Windows 2000 and Windows 2003. Web modules exist for IIS5 and IIS6 to protect Citrix Nfuse, Web Interface, Secure Gateway, Secure Access Manager (Form-based authentication) and Outlook Web Access 2000 and 2003 (Basic Authentication).

Support for ODBC databases and Active Directory

Any ODBC compliant database can be used instead of the default MS Access Database (MS SQL Server, Oracle). Active Directory can also be used as a repository. This option requires an AD schema update.

Online Licensing

An online licensing mechanism is used to allow automatic delivery of a license file by e-mail.

Authentication Methods

Different authentication methods can be set on server level and on user level: local (VM only), proxy (back-end RADIUS server only), Windows (Windows domain controller only), local and proxy, local and Windows. On top of that Default (server level authenticator will be used) and Disabled (user can not log on) can be used on user level. Using proxy or Windows is also known as pass-through.

8.2 Deployment

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

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.

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.

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.

Token Self Assign

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

Token Auto Assign

Allows automatic assignment of the first available token to a user on user creation. An e-mail with the serial number of the token and the name of the user can be sent to an administrator.

Grace Period

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

Bulk Management

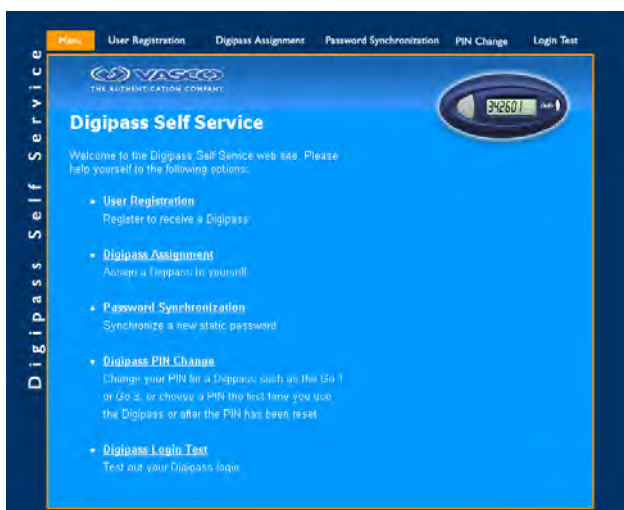
Allows administrators to quickly administer multiple users and tokens with a single mouse click.

CSV File Import

A comma separated file (.csv) can be created containing users, serial numbers of Digipasses and other information. By importing this file into the VACMAN Middleware, the users are created, the Digipasses are assigned and other settings are determined.

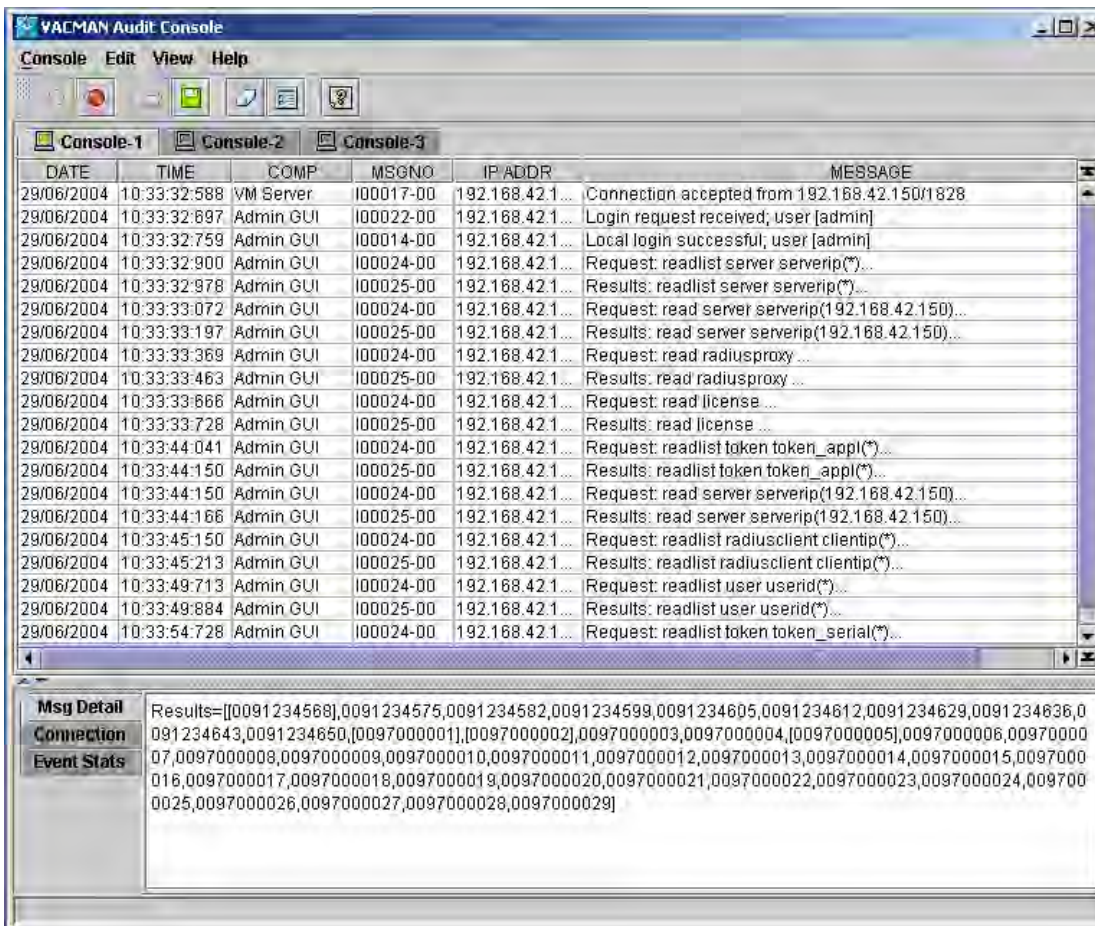
User Self Management Web Site

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 token self assign, to update their back-end password stored in the VM database, to do a change PIN (Go-1/Go-3 token), to do a token test.



8.3 Administration

A highly intuitive graphical user interface (GUI) 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 and require a Java Runtime Environment (JRE) to be installed.



8.4 Advanced Features

Protocol Support - PAP, CHAP, MS-CHAP v1, MS-CHAP v2, MPPE are supported by the VM. This means that PPTP is also supported. Some features of VM are not or only partially supported when using CHAP or MS-CHAP: Windows Authentication, Password Autolearn, Token Self Assign, Change PIN, Stored Password Proxy, Challenge/Response. The User Self Management Web Site can be used to overcome these drawbacks.

Redundancy, Failover and Replication - A Primary and a Backup VM can be installed and a built-in database replication feature assures databases are in sync. This allows for some form of redundancy – failover. The replication process will automatically attempt re-connection until connection is restored. When using the Active Directory option the AD replication can be used instead of the built-in VM database replication. The same is true for ODBC compliant databases (SQL Server, Oracle).

9 Conclusion

NETASQ IPS-Firewall together with DIGIPASS authentication solutions provides secure remote access to your internal network resources.

10 For more information on NETASQ

To find your nearest NETASQ partner or to contact NETASQ please go to:

www.NETASQ.com

11 For more information on VASCO

To find more information about VASCO please visit www.vasco.com and click on “where to buy” to locate the nearest VASCO partner in your region.

12 About NETASQ

Created in 1998, NETASQ is a European company which develops and markets innovative IPS firewall and VPN security solutions for all types of companies: small-to-medium sized firms, large enterprises and government agencies. NETASQ has full control over its proprietary in-line Intrusion Prevention technology: ASQ (Active Security Qualification), thereby ensuring its customers the longevity required for best-of-breed security appliances which adapt to the ever-changing risks faced by information systems. NETASQ distributes its products via a network of partners, including distributors, ISPs, approved VARs, retailers and integrators.

13 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.

With over 10 million current users of its DIGIPASS products, VASCO has established itself as a world leader for Strong Authentication with over 250 international financial institutions, approximately 1200 blue-chip corporations, and governments representing more than 60 countries.