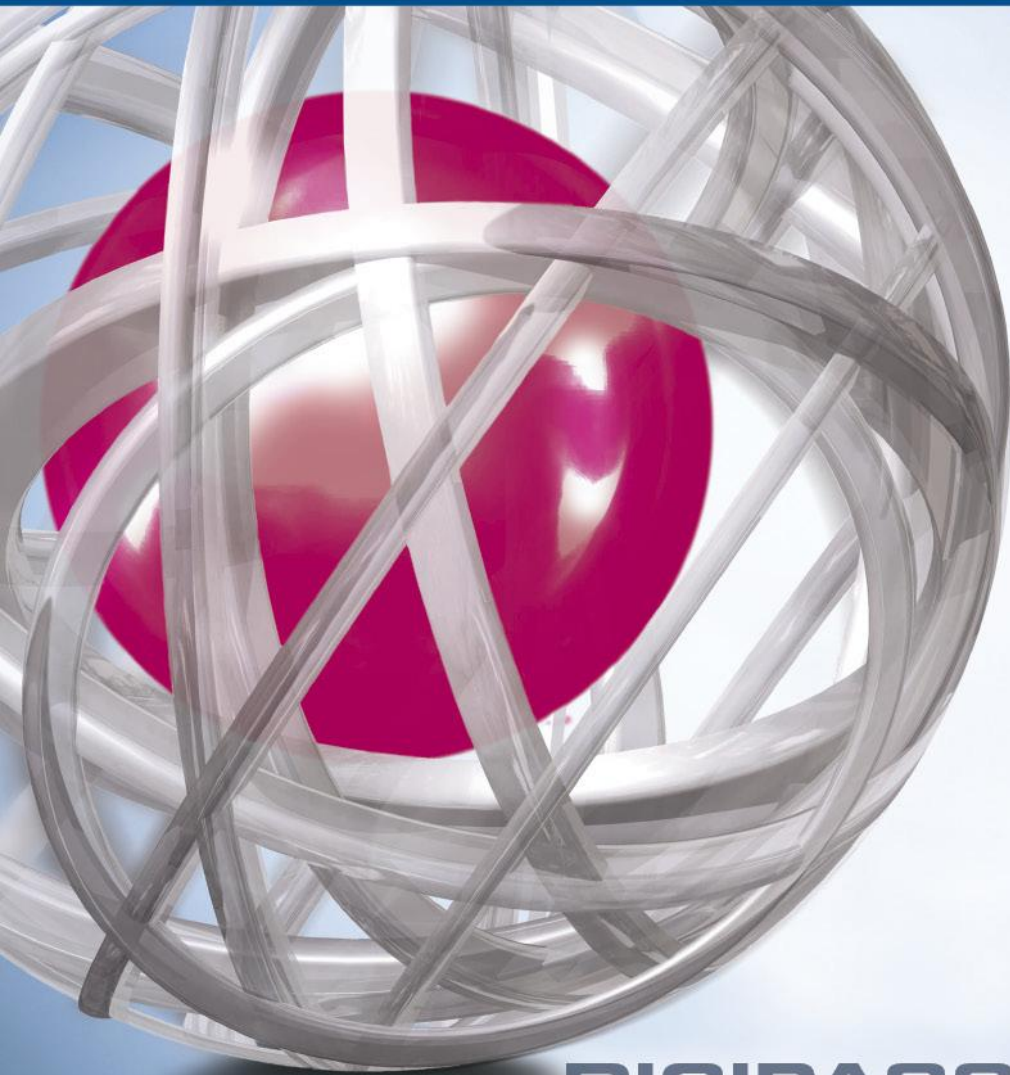




# DIGIPASS Authentication for VMware View



**DIGIPASS BY VASCO**



The world's leading software company specializing in **Internet Security**


# Disclaimer

## Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

## Copyright

Copyright © 2012 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXsGUARD™™, DIGIPASS® and  logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.



# Table of Contents

<b>Reference guide .....</b>	<b>3</b>
<b>1 Technical Concepts .....</b>	<b>4</b>
1.1 VMware.....	4
1.1.1 View.....	4
1.2 VASCO.....	4
1.2.1 IDENTIKEY Authentication Server.....	4
<b>2 VMware View RADIUS authentication .....</b>	<b>5</b>
2.1 Architecture.....	5
2.2 Prerequisites.....	5
2.3 VMware View .....	5
<b>3 Identikey Authentication Server setup .....</b>	<b>8</b>
3.1 IDENTIKEY Authentication Server.....	8
3.1.1 Policies .....	8
3.1.2 Client .....	9
3.1.3 User .....	10
3.1.4 DIGIPASS .....	10
<b>4 Test the solution .....</b>	<b>12</b>
<b>5 FAQ.....</b>	<b>13</b>
<b>6 Appendix.....</b>	<b>13</b>



# Reference guide

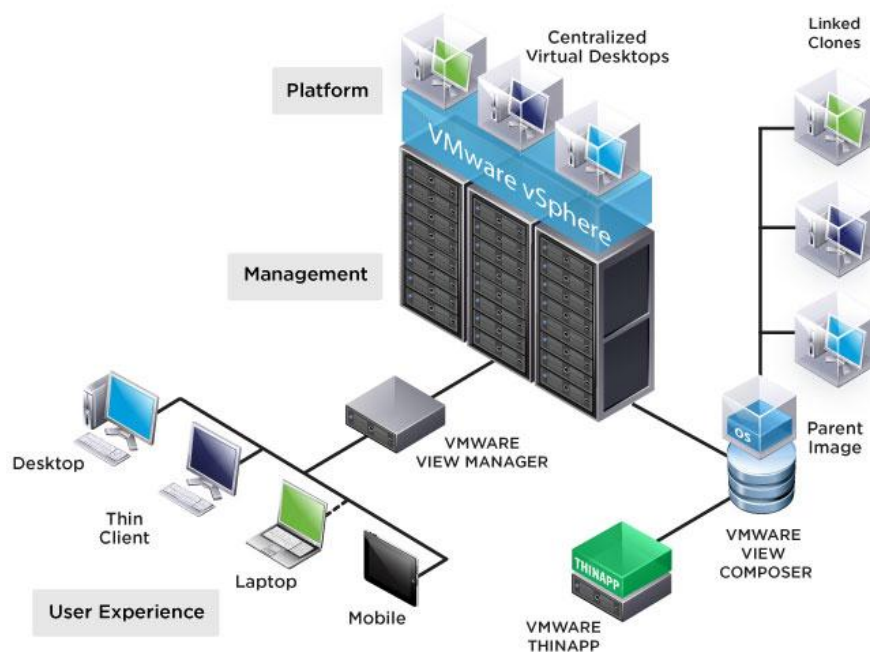
ID	Title	Author	Publisher	Date	ISBN

# 1 Technical Concepts

## 1.1 VMware

### 1.1.1 View

Simplify desktop and application management while increasing security and control with VMware View. Deliver a personalized high fidelity experience for end-users across sessions and devices. Enable higher availability and agility of desktop services unmatched by traditional PCs while reducing the total cost of desktop ownership up to 50%. End-users can enjoy new levels of productivity and the freedom to access desktops from more devices and locations while giving IT greater policy control.



## 1.2 VASCO

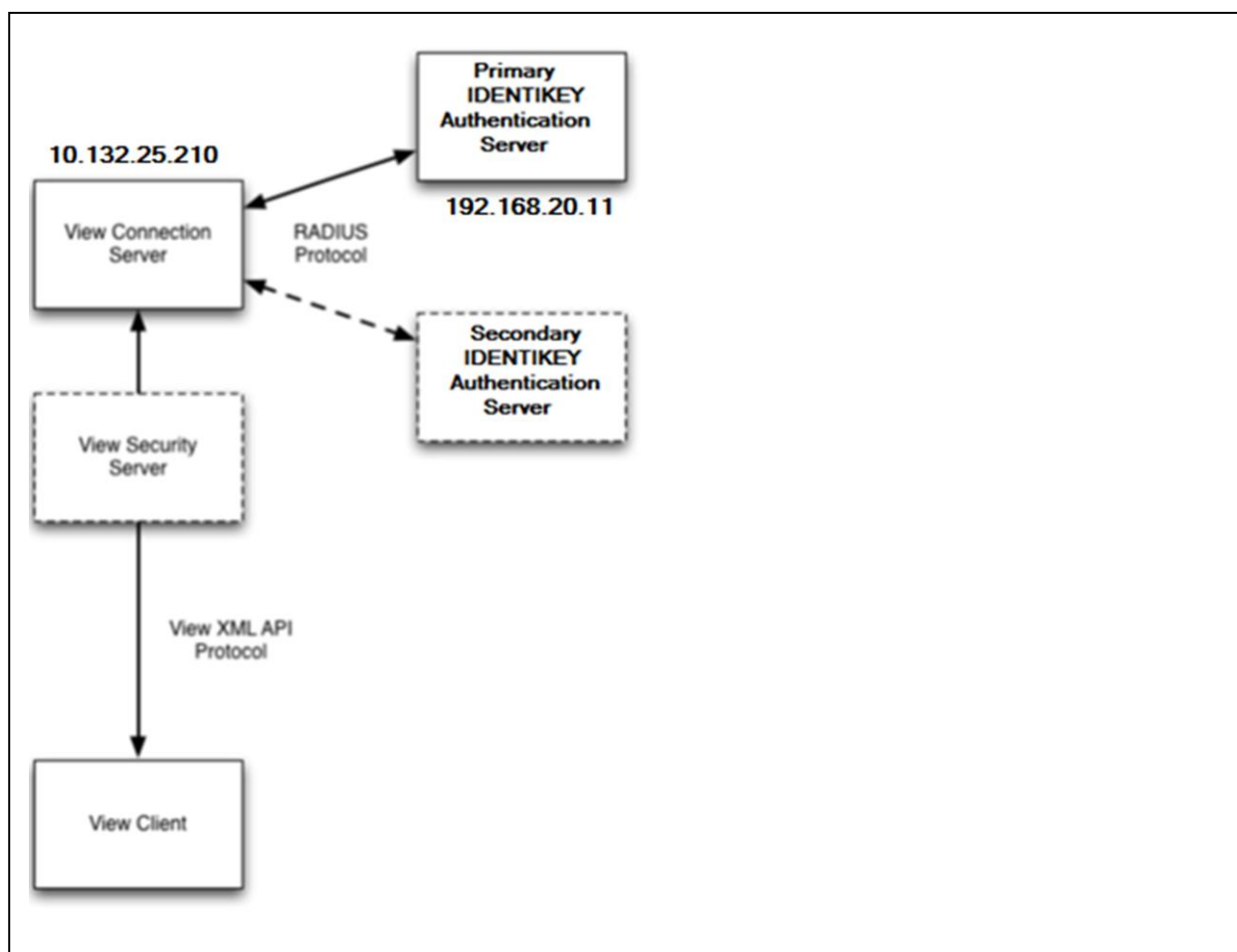
### 1.2.1 IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

IDENTIKEY Server is supported on 32bit systems as well as on 64bit systems.

## 2 VMware View RADIUS authentication

### 2.1 Architecture



### 2.2 Prerequisites

The minimum test setup for View RADIUS authentication is a single View Connection Server, a single RADIUS server and a single View Client as shown in the diagram above. A secondary RADIUS server, View Security Servers and replica Connection Servers are optional.

### 2.3 VMware View

Set up an IDENTITYKEY Authentication Server as a RADIUS Server for requests from the View Connection Server.

Install View Connection Server (standard instance) on a Windows Server 2008 R2 system. Use View Connection Server version 5.1 or newer.

From a Web browser, access View Administrator on the Connection Server using <https://hostname/admin> and log in.



The screenshot shows the 'Edit View Connection Server Settings' dialog box with the 'Authentication' tab selected. The 'Smart card authentication' is set to 'Optional'. Under 'Advanced Authentication', '2-factor authentication' is set to 'RADIUS'. The 'Authenticator' is set to 'Identikey'. There are checkboxes for 'Disconnect user sessions on smart card removal', 'Enforce 2-factor and Windows user name matching', and 'Use same username and password for RADIUS and Windows authentication'. A 'Manage Authenticators...' button is at the bottom.

4. Under View Configuration > Servers > Connection Servers select the Connection Server

Click **Edit**

Select **Authentication**

- 2-Factor authentication: **RADIUS**
- Authenticator: Create New **Authenticator**

Click **OK**

The screenshot shows the 'Edit RADIUS Authenticator' dialog box with the 'Primary Authentication Server' tab selected. The 'Label' is 'Digipass' and the 'Description' is 'Identikey'. Under 'Primary Authentication Server', the 'Hostname/Address' is '192.168.20.11', 'Authentication port' is '1812', 'Accounting port' is '1813', 'Authentication type' is 'PAP', 'Shared secret' is '\*\*\*\*\*', 'Server timeout' is '3' seconds, 'Max retries' is '5', 'Realm prefix' is empty, and 'Realm suffix' is empty.

- Label: **Identikey**
- Hostname/Address: **192.168.20.11** (IP-address of Identikey Authentication Server)
- Authentication port: **1812**
- Accounting port: **1813**
- Authentication Type: **PAP**



- Shared secret: **Test123**
- Server timeout: **3**
- Max retries: **5**

Click **Next**



If there is a secondary RADIUS server then complete the settings for the secondary server.

Click **Finish**





## 3 Identikey Authentication Server setup

### 3.1 IDENTIKEY Authentication Server

There are lots of possibilities when using IDENTIKEY Authentication Server. We can authenticate with:

- Local users (Defined in IDENTIKEY Authentication Server)
- Active Directory (Windows)

For VMware View we only need the Local authentication of the DIGIPASS. Active Directory Credentials are verified with the standard verification procedure VMware View.

#### 3.1.1 Policies

In the Policy the behavior of the authentication is defined. It gives all the answers on: I have got a user and a password, what now?

- **Create** a new Policy



Create new Policy

Create a policy by completing the details below. \* indicates mandatory fields.

Policy ID \*

Description

Inherits From

- Policy ID : **VMWARE View**
- Inherits From: **Base Policy**



Inherits means: The new policy will have the same behavior as the policy from which he inherits, except when otherwise specified in the new policy.



Example:

	Base Policy	New Policy	Behaviour
1	a		New policy will do <b>a</b>
2	b		New policy will do <b>b</b>
3	c	f	New policy will do <b>f</b>
4	d		New policy will do <b>d</b>
5	e	g	New policy will do <b>g</b>

The new policy is created, now we are going to edit it.

[Click here to manage](#)

- Click **edit**

- Local Authentication : **Digipass/Password**
- Click **Save**

### 3.1.2 Client

In the clients we specify the location from which IDENTIKEY Authentication Server will accept requests and which protocol they use.

We are going to add a new RADIUS client.

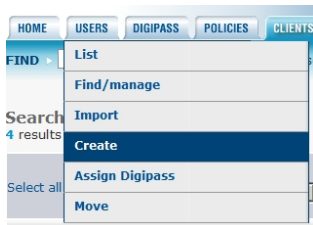
- Client Type : select **Radius Client** from “**select from list**”
- Location : **10.132.25.210** (IP-Address of the VMware View connection server)
- Policy ID : Select the Policy that was created in [Policies](#)



- Protocol ID: **RADIUS**
- Shared Secret: **Test123**
- Confirm Shared Secret: reenter the **shared secret**
- Click **Save**

### 3.1.3 User

We are going to create a user.



Create new User

Create a user by completing the details below. \* indicates mandatory fields.

User ID \*

Domain \*

Organizational Unit

Enter static password

Confirm static password

Local Authentication

Back-End Authentication

Disabled ☐

Locked ☐

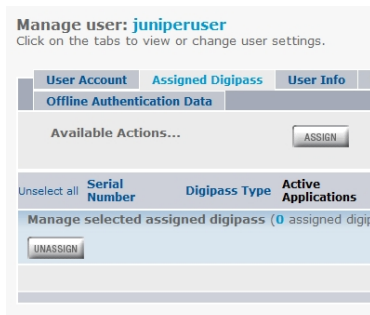
Expiration Date

- User ID: **VMware\_user**

### 3.1.4 DIGIPASS

The purpose of using IDENTIKEY Authentication Server, is to be able to log in using One Time Passwords (OTP). To make it possible to use OTP we need to assign a DIGIPASS to the user. The Digipass is a device that generates the OTP's.

- Open the user by clicking on its name
- Select **Assigned Digipass**



- Click **ASSIGN**



Application Name: [text box]

Application Type: [Any] [v]

☐ Search upwards in the organizational hierarchy

On clicking NEXT:

☒ Search and auto-select during assignment

Description: [text box]

Results per page (10~100): [10]

[NEXT] [CANCEL]

- Click **Next**

**Assign Digipass**

Follow the steps below to select users and assign them Digipass.

1. Search Digipass 2. Select Digipass 3. Options 4. Finish

**Assign Digipass Summary**

No. of Users selected: 1

No. of Digipass found matching the selection criteria: auto-select next available

**Assignment Options**

Grace period: [0] Days [v]

Verify the selected options and click Assign to proceed assigning the Digipass. Click Cancel to abort the assign Digipass operation.

[ASSIGN] [CANCEL]

- Grace period: **0 Days**



Grace period is the period that a user can log in with his static password. The first time the user uses his DIGIPASS the grace period will expire.

- Click **ASSIGN**



**Assign Digipass**

Follow the steps below to select users and assign them Digipass.

1. Search Digipass 2. Select Digipass 3. Options 4. Finish

**Task completed!** You have assigned 1 Digipass, as summarized below.

Select all	Serial Number	Digipass Type	Active Applications	UserID
<input type="checkbox"/>	0091234568	DPG03	APPL1 1	juniperuser

0 digipass selected

MORE actions...

[For these Users...]

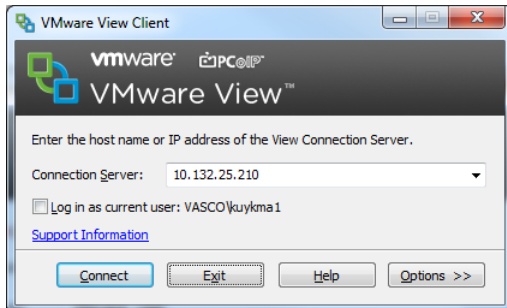
[FINISH]

- Click **Finish**



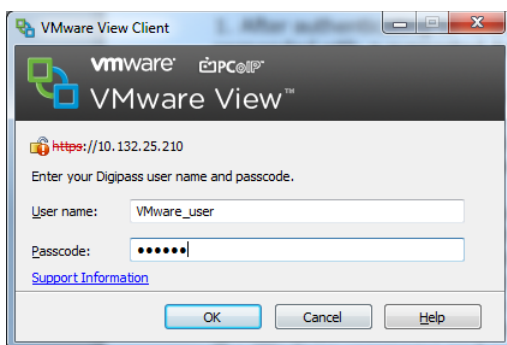
## 4 Test the solution

Download the VMware View Client from the VMWare website. (<https://my.vmware.com/>)



- Connection Server: **10.132.25.210**

Click **Connect**



User name: **VMware\_user**

Passcode: **OTP generated by you Digipass**



After authenticating to RADIUS, you may get another prompt if the RADIUS server responded with a supported Access Challenge.



Enter you **Digipass** user and passcode  
**Digipass** is the label provided in "edit radius authenticator" (p. 6)



## 5 FAQ

1. In the admin configuration of RADIUS authentication under Advanced Authentication, if Enforce 2-factor and Windows user name matching is ticked then the Windows login prompt after RADIUS authentication will force the username to be the same as the RADIUS username and the user will not be able to modify this.
2. Similarly if Use same username and password for RADIUS and Windows authentication is ticked then the user will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication used Windows username and password. This feature is used in cases where the initial RADIUS authentication uses Windows authentication which triggers an out-of-band transmission of a DIGIPASS OTP which is used as part of a RADIUS challenge. This then avoids the need for the user to re-enter the Windows username and password after RADIUS authentication. This feature will not work in Windows View clients older than 5.1.

## 6 Appendix