DIGIPASS Authentication for
Juniper MAG Series Junos Pulse Gateways

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 © 2014 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.
# Table of Contents

**Reference guide** ............................................................................................................. 4

1 Overview ................................................................................................................................ 5

2 Technical Concepts ........................................................................................................... 6

2.1 Microsoft ........................................................................................................................... 6

2.1.1 Windows Server ........................................................................................................... 6

2.2 Juniper ............................................................................................................................... 6

2.2.1 MAG Series Junos Pulse Gateways ........................................................................... 6

2.3 VASCO .............................................................................................................................. 6

2.3.1 IDENTIKEY server or aXsGUARD Identifier .............................................................. 6

3 Setup – without IDENTIKEY ............................................................................................ 7

3.1 Architecture ...................................................................................................................... 7

3.2 Juniper ............................................................................................................................... 7

3.2.1 Authentication Servers ................................................................................................. 7

3.2.2 User Realms .................................................................................................................. 8

3.2.3 User Roles .................................................................................................................... 8

3.2.4 Sign-in .......................................................................................................................... 9

3.3 Test the Setup ................................................................................................................... 9

4 Solution .................................................................................................................................. 11

4.1 Architecture ...................................................................................................................... 11

4.2 Juniper ............................................................................................................................... 11

4.2.1 Authentication Servers ................................................................................................. 11

4.2.2 User Realms .................................................................................................................. 11

4.2.3 Sign-in page .................................................................................................................. 12

4.3 IDENTIKEY Server .......................................................................................................... 12

4.3.1 Policies .......................................................................................................................... 13

4.3.2 Client .............................................................................................................................. 14
DIGIPASS Authentication for Juniper MAG Series Junos Pulse Gateways

4.3.3 User ........................................................................................................................................... 15
4.3.4 DIGIPASS .................................................................................................................................. 15
4.4 Test the Solution ............................................................................................................................ 17

5 Solution - Virtual DIGIPAS ............................................................................................................. 18
5.1 Architecture ................................................................................................................................. 18
5.2 Juniper .......................................................................................................................................... 19
  5.2.1 Authentication Servers .......................................................................................................... 19
5.3 VASCO .......................................................................................................................................... 20
  5.3.1 SMS gateway ......................................................................................................................... 20
  5.3.2 IDENTIKEY Server ................................................................................................................. 21
5.4 Test the Solution ............................................................................................................................ 23

6 FAQ .................................................................................................................................................. 25

7 Appendix .......................................................................................................................................... 25
## Reference guide

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Author</th>
<th>Publisher</th>
<th>Date</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1 Overview

This whitepaper describes how to configure a Juniper MAG Series Junos Pulse Gateways in combination with the VASCO IDENTIKEY Server. The combination of those two products makes it possible to set up a secure remote connection between the outside world and the company’s internal network.
2 Technical Concepts

2.1 Microsoft

2.1.1 Windows Server

In this configuration we used Windows 2008 Server. Windows 2012 or any other server with below features are supported as well. This server can play different roles, like there are:

- Domain Controller
- Web Server
- Mail Server
- ...

2.2 Juniper

2.2.1 MAG Series Junos Pulse Gateways

MAG Series Junos Pulse Gateways enable dynamic policy-driven security enforcement with Junos Pulse client, Junos Pulse Secure Access Service (SSL-VPN), and Junos Pulse Access Control Service (UAC) that provides market-leading secure, segmented remote and local network access on a single platform.

They enable authorized users, including employees, telecommuters, mobile workers, contractors, guests, customers, and more, to have safe, secure remote and LAN-based network access. A range of models offers flexible deployment for all sizes of business networks, and support broad coverage across mobile and non-mobile devices, with built-in device integrity checking to further enable enterprise BYOD initiatives.

Junos Pulse Secure Access Service on MAG Series creates a simplified user experience for consistent, secure, remote and extensible access to corporate network and cloud resources. It supports Single sign-on (SSO), Windows 8, HTML 5, and WebSockets, and enables secure, identity-, device-, and location-based network and application access control across multiple device types.

2.3 VASCO

2.3.1 IDENTITY Server or aXsGUARD Identifier

IDENTIKEY 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.

aXsGUARD Identifier is a standalone authentication appliance that secures remote access to corporate networks and web-based applications.

⚠️ The use and configuration of an IDENTITY Server and an aXsGUARD Identifier is similar.
3 Setup – without IDENTIKEY

Before adding 2 factor authentication it is important to validate a standard configuration without One Time Password (OTP).

3.1 Architecture

3.2 Juniper

3.2.1 Authentication Servers

In order to authenticate using Active Directory, we need to add an authentication server with the specifications of Active Directory.

- **Name**: fill in a **meaningful name**
- **Primary Domain Controller**: The **IP address** of the **Domain Controller**
- **Backup Domain Controller**: The **IP address** of the **Backup Domain Controller** *(Optional)*
- **Domain**: The **domain** to which the Domain Controller belongs.
- **Enable Allow domain to be specified as part of username**
  - Ex: domain\user1
- **Enable Allow trusted domains**
- **Admin Username**: Enter a **username** of a user that has **admin privileges** in Active Directory
3.2.2 User Realms

The User Realm is used to specify which authentication server has to be used in order to authenticate a user.

- Name: fill in a meaningful name
- Description: fill in a meaningful description
- Authentication: Select the Authentication Server that is specified in 3.1.1 Auth. Servers
- Directory/Attribute: Same as above
- Accounting: None
- Save

3.2.3 User Roles

According to specified criteria users can have different roles. For example

- Click on the Role Mapping tab
- New Rule
- Select Rule based on Group membership and click Update
- Click on Groups to get the Group selection popup
- Click on Search
- You will see a list of all your Active Directory groups
- Check the box for the groups that you want to use in Juniper SSL VPN and click Add Selected on top.
- Click OK
- In Rule... If users is a member of any of these selected groups >> Select one or more groups and click the “Add” button.
- ... then assign these roles >> select the Juniper role you want to assign to these groups (you will need to create roles before you start!)
- Save Changes
### 3.2.4 Sign-in

Now we have to select which realm we want to use to Sign in on our VPN website.

![Sign-in configuration screen](image)

### 3.3 Test the Setup

Browse to the SSL VPN Web portal, this would be the IP address of the juniper appliance.

![SSL VPN Web portal](image)

Username: a **user** known in the Active Directory specified in 3.2.1 Authentication Servers

Password: the **password** of the Active Directory user
4 Solution

4.1 Architecture

4.2 Juniper

4.2.1 Authentication Servers

In order to authenticate using IDENTIKEY server we need a new RADIUS authentication server

<table>
<thead>
<tr>
<th>Settings</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>IDENTKEY</td>
</tr>
<tr>
<td>NAS-Identifier:</td>
<td>fill in a meaningful name</td>
</tr>
<tr>
<td>Primary Server</td>
<td></td>
</tr>
<tr>
<td>Radius Server:</td>
<td>10.132.224.202</td>
</tr>
<tr>
<td>Authentication Port:</td>
<td>1812</td>
</tr>
<tr>
<td>Shared Secret:</td>
<td>Enter a secret word</td>
</tr>
<tr>
<td>Accounting Port:</td>
<td>Standard 1813</td>
</tr>
<tr>
<td>NAS-IP-Address:</td>
<td>The IP address of the Juniper box (Intern)</td>
</tr>
<tr>
<td>Timeout:</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Retries:</td>
<td>0</td>
</tr>
</tbody>
</table>

Notes: if you select this, the device will send the user’s authentication method as “token” if you use SAML, and this credential will not be used in automatic SSO to backend applications.

- Name: fill in a meaningful name
- NAS-Identifier: The name of the Juniper box known to the network
- Radius Server: The IP adres of the IDENTIKEY Server
- Authentication Port: Standard 1812
- Shared Secret: Enter a secret word
- Accounting Port: Standard 1813
- NAS-IP-Address: The IP adres of the Juniper box (Intern)
- Enable Users authenticate using tokens or one-time passwords
- Save

4.2.2 User Realms

Now we have to specify a new user realm where we will link the new Authentication Server.
• Name: fill in a **meaningful name**
• Description: fill in a **meaningful description**
• Authentication: Select the **Authentication Server** that is specified in 4.1.1 **Auth. Servers**
• Directory/Attribute: **Same as above**
• Accounting: **None**
• Save

### 4.2.3 Sign-in page

Now we have to link our new user realm to the Sign-in page

![Sign-in page](image)

It is possible to select multiple realms. This will give a select list on the Sign-in page with the multiple possibilities.

### 4.3 IDENTIKEY Server

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

• Local users (Defined in IDENTIKEY)
• Active Directory (Windows)
• …

In this whitepaper we will use Local users to authenticate.
4.3.1 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](image)

- **Policy ID**: Fill in a meaningful name
- **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:

<table>
<thead>
<tr>
<th>Base Policy</th>
<th>New Policy</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 a</td>
<td></td>
<td>New policy will do <strong>a</strong></td>
</tr>
<tr>
<td>2 b</td>
<td>f</td>
<td>New policy will do <strong>b</strong></td>
</tr>
<tr>
<td>3 c</td>
<td>f</td>
<td>New policy will do <strong>f</strong></td>
</tr>
<tr>
<td>4 d</td>
<td>g</td>
<td>New policy will do <strong>d</strong></td>
</tr>
<tr>
<td>5 e</td>
<td>g</td>
<td>New policy will do <strong>g</strong></td>
</tr>
</tbody>
</table>

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

- **Click** edit

[Click here to manage Juniper Test]
Local Authentication: Digipass/Password  
Save

4.3.2 Client

In the clients we specify the location from which IDENTIKEY 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: Fill in the IP Address of the Juniper box
- Policy ID: Select the Policy that was created in 4.2.1 Policies
- Protocol ID: RADIUS
- Shared Secret: same word as entered in 4.1.1 Auth. Servers
- Confirm Shared Secret: reenter the shared secret
- Save
4.3.3 User
In order to login to the VPN/SSL we need a user.

We are going to create a user.

- User ID: Fill in the **username**
- Enter static password: Fill in a **password**

Password is used when there is no Digipass assigned.

- Confirm static password: **Confirm the password**

4.3.4 DIGIPASS
The purpose of using IDENTIKEY Servers, 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.

There are several ways to link a Digipass to a User. Here we are assigning a Digipass we start selecting a User. (assuming the Digipasses are already loaded into IDENTIKEY Server)

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

- Click **ASSIGN**
• Click **Next**

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**

**Assigning Digipass**

Please wait...

• Click **Finish**
4.4 Test the Solution

Browse to the SSL VPN Web portal, this would be the IP address of the juniper appliance

Username: JuniperUser created in 4.2.3 User

Password: OTP generated by the Digipass linked to that user
5 Solution - Virtual DIGIPAS

5.1 Architecture

Juniper can also be configured to use Virtual Digipass. Virtual Digipass is a solution where the OTP is sent via mail or SMS. The user only needs his mobile phone, no other device or installation is needed.

The following prerequisites have to be confirmed on the IDENTIKEY Server:

- Digipasses in IDENTIKEY Server are Virtual Digipasses OR have Virtual Back Up Digipas enabled
- SMS gateway has to be enabled and configured
  - If you want to use SMS as delivery method
- Mail server has to be enabled and configured
  - If you want to use E-mail as delivery method
- The users mobile phone number has to be filled in to IDENTIKEY Server

In this document we will use an **SMS gateway**.
5.2 Juniper

5.2.1 Authentication Servers

In order to authenticate using virtual Digipass we have to modify the settings of the radius authentication server (IDENTIKEY).

- Open the authentication server called IDENTIKEY
- Scroll down to Custom Radius Authentication Rules

- Click New Radius Rule
- A Pop-up will appear

Fill in following settings:

- Incoming Packet Type: Access Challenge
- Radius Attribute: Reply-Message (18)
- Operand: matches the expression
- Value: enter One-Time Password
- Then take action ...: show NEXT TOKEN page
- Click Save Changes
- Also save changes for the authentication server

Juniper will show an extra webpage (login-page) when this rule is triggered. The Trigger is a standard radius attribute that is returned by the radius server (IDENTIKEY).
5.3 VASCO

5.3.1 SMS gateway

Start > all programs > VASCO > IDENTIKEY Server > Virtual DIGIPASS MDC Configuration

- **Select** SMS Delivery

- **Fill in the gateway information**

There are several SMS gateway providers. Settings are different depending on the provider.

Providers can be:

http://www.clickatell.com

http://www.tyntec.com/

...
5.3.2 IDENTIKEY Server

Now that we have configured the SMS gateway, we have to edit the policy. We have to enable the function Virtual Digipass and define a trigger.

Go to Start > all programs > VASCO > IDENTIKEY Server > IDENTIKEY Web admin

- **Login**
- **Select Policies > List**

- Select the **policy** that is used in combination with Juniper
- Go to **Virtual Digipass**
There are two kinds of Virtual Digipasses:

1. **Primary Virtual Digipass**: A Primary Virtual Digipass is handled similarly to a standard physical Digipass. It is imported into the IDENTIKEY server, assigned to a User, and treated by the IDENTIKEY server as any other kind of Digipass. Also a Primary Virtual Digipass has its own serial number.

2. **Backup Virtual Digipass**: The Backup Virtual Digipass is meant as a back-up system for a forgotten/stolen/broken standard Digipass. The Backup Virtual Digipass has not its own serial number, but is a feature that can be enabled on a standard Digipass.

- **Delivery Method**: Select SMS
- **Primary Virtual Digipass**: Only possible when Virtual Digipass was ordered
- **Request Method**: Password

  This is the trigger: When the user enters his static password in the password field, an SMS will be sent to his mobile phone.

- **Backup Virtual Digipass**: Only possible when Backup Virtual Digipass is enabled
- **BVDP Mode**: Yes - Permitted
- **Request Method**: Keyword
- **Request Keyword**: sendotp

  This is the trigger: When the user enters sendotp in the password field, an SMS will be sent to his mobile phone.

- **Save**

  In both cases IDENTIKEY server will return a standard RADIUS attribute (Reply-Message (18)) with the value: "**enter One-Time Password**", to the requesting client. The client can trigger special behavior when this attribute is returned (Like we do in 5.2.1 Authentication servers).
• **Mobile**: Fill in the mobile number of the user

  Must contain a phone number that consists of only numbers, spaces and brackets ( ) {}. There may also be a + at the beginning of the number. A maximum of 20 characters can be entered here.

• **Save**

### 5.4 Test the Solution

Browse to the application, this would be the IP address of the juniper appliance
DIGIPASS Authentication for Juniper MAG Series Junos Pulse Gateways

- Username: JuniperUser created in 4.2.3 User
- Password: Static password (when Virtual Digipass is linked to the user)

Or
- Password: sendotp (when Backup Virtual Digipass is enabled)
- An SMS will be send to the mobile phone, containing an OTP
- An new webpage is asking for the OTP

- Fill in OTP
6 FAQ
7 Appendix