Juniper Two Stage Challenge and Response

Contents

- 1 Juniper Two Stage and Challenge and Response Authentication
- 2 Introduction
- 3 Prerequisites
- 4 Baseline
- 5 Architecture
- 6 Installation
- 7 Adding Two Stage Authentication
- 8 Adding Challenge and response Authentication
- 9 Combining Juniper and PINsafe Two Stage Authentication
- 10 Verifying the Installation
- 11 Troubleshooting
- 12 Known Issues and Limitations
- 13 Additional Information

Juniper Two Stage and Challenge and Response Authentication

Introduction

Juniper supports the use of a challenge and response whereby a password is used prior to entering a One Time Code. In addition the Challenge and Response mechanism allows an SMS to be sent upon successful entry of a password.

Prerequisites

PINsafe 3.7

Juniper 6.x

Dual Channel authentication

Two stage authentication requires the use of either a PINsafe password, or that Check password with repository is enabled.

Baseline

PINsafe 3.7

Juniper 6.4

Architecture

Juniper using RADIUS authentication to the PINsafe server, with security strings sent to the user using an SMS gateway.

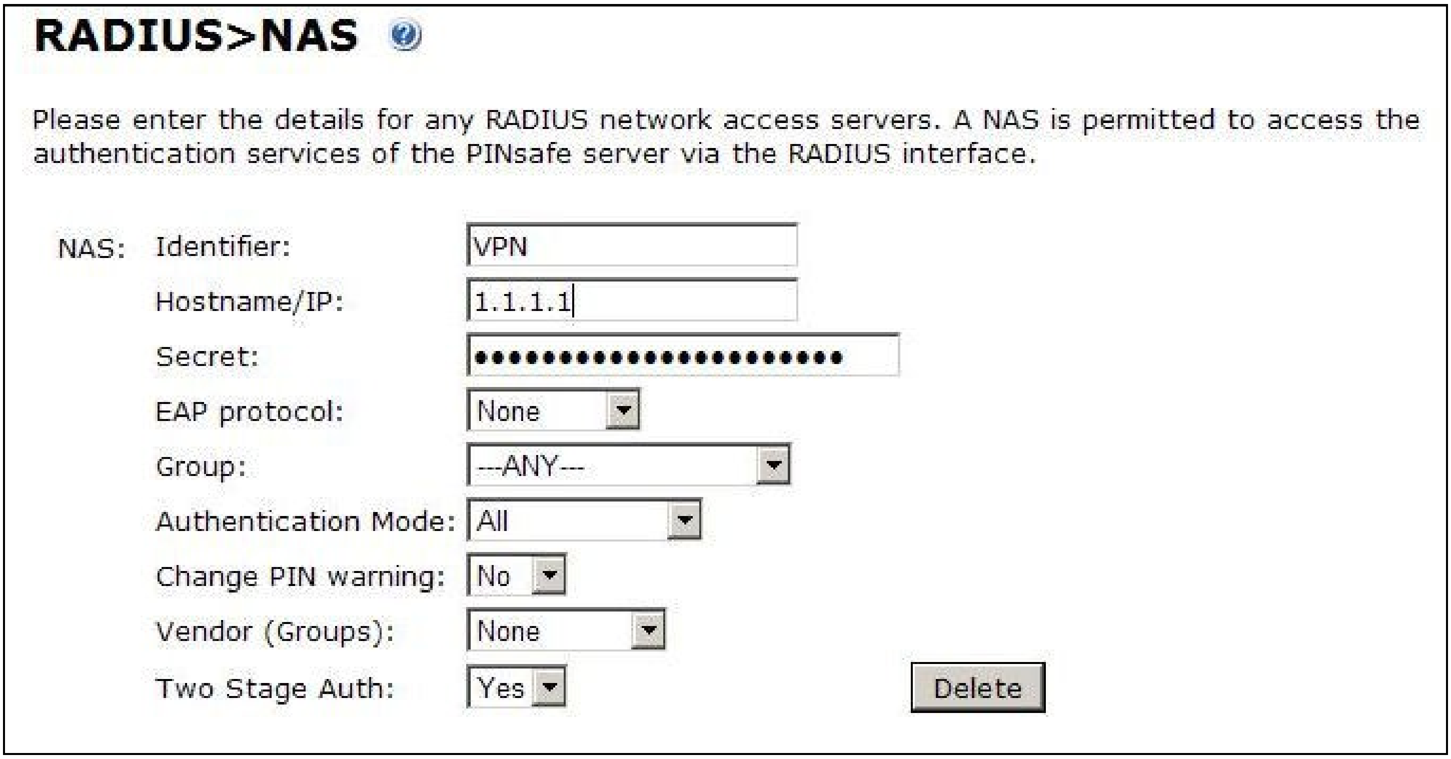
Installation

Configure the PINsafe server and Juniper appliance for Dual Channel Authentication. Ensure either the user has a PINsafe password, or that Check password with repository is enabled.

Adding Two Stage Authentication

See also: Two Stage Authentication How to Guide

On the PINsafe Administration Console server select RADIUS/NAS and the Access device which two stage authentication is required. Set the Two stage Auth to Yes and Apply.

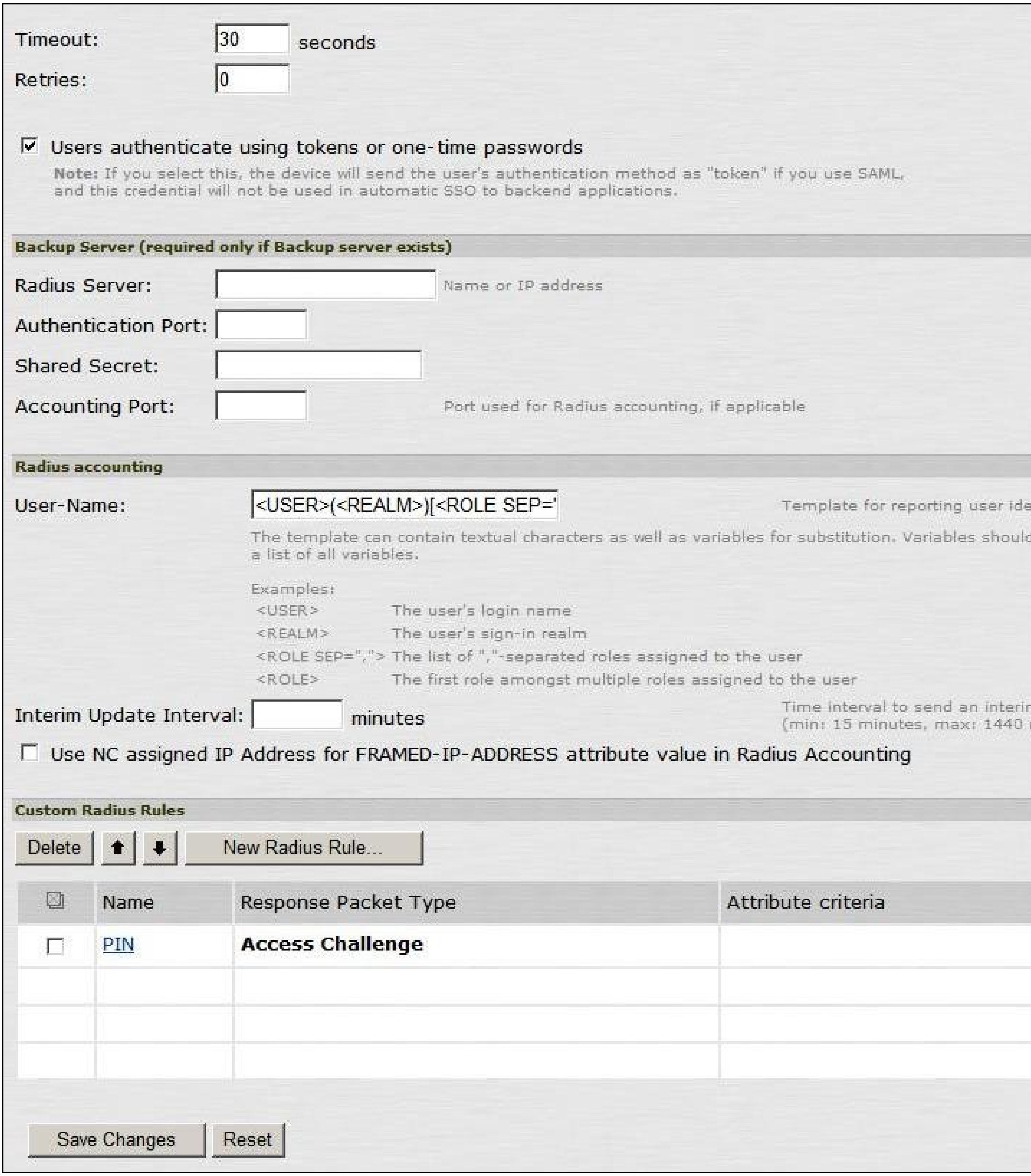


RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the PINsafe server via the RADIUS interface.

NAS:	Identifier:	VPN
	Hostname/IP:	1.1.1.1
	Secret:	••••••••••••••••••••••
	EAP protocol:	None
	Group:	---ANY---
	Authentication Mode:	All
	Change PIN warning:	No
	Vendor (Groups):	None
	Two Stage Auth:	Yes

On the Juniper Administration Console, browse to the Authentication/Auth Servers menu, and select the PINsafe RADIUS authentication server. Under Custom RADIUS Rules click on the New RADIUS Rule button.



Timeout: 30 seconds

Retries: 0

☑ Users authenticate using tokens or one-time passwords

Note: 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.

Backup Server (required only if Backup server exists)

Radius Server: Name or IP address

Authentication Port:

Shared Secret:

Accounting Port: Port used for Radius accounting, if applicable

Radius accounting

User-Name: <USER>(<REALM>)[<ROLE SEP=' Template for reporting user ide

The template can contain textual characters as well as variables for substitution. Variables shoul a list of all variables.

Examples:	
<USER>	The user's login name
<REALM>	The user's sign-in realm
<ROLE SEP=",">	The list of ","-separated roles assigned to the user
<ROLE>	The first role amongst multiple roles assigned to the user

Interim Update Interval: minutes Time interval to send an interir (min: 15 minutes, max: 1440

□ Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute value in Radius Accounting

Custom Radius Rules

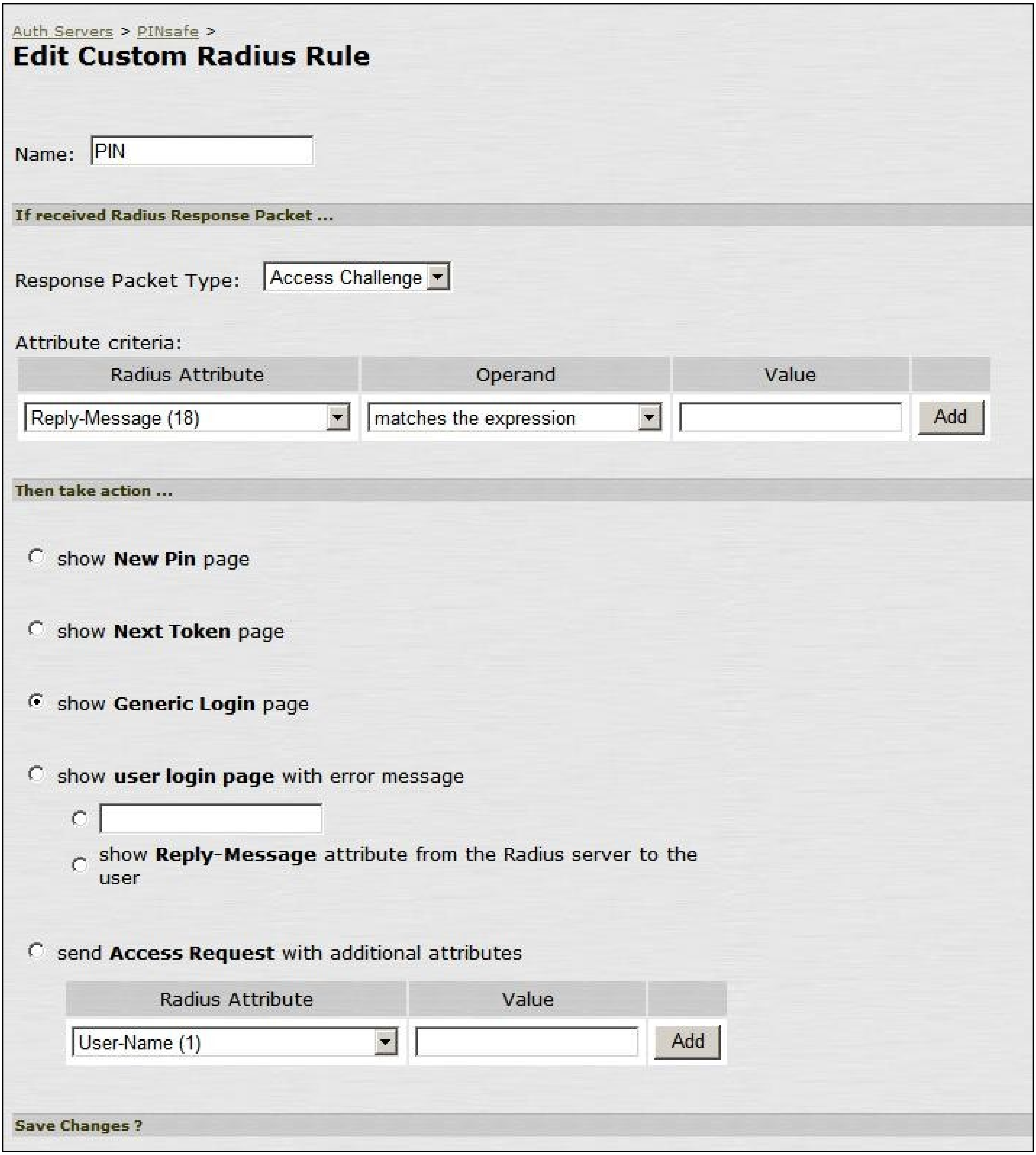
☒	Name	Response Packet Type	Attribute criteria
□	PIN	**Access Challenge**	

Enter a name for the Rule and ensure Response Packet Type is set to Access Challenge.

Under Attribute Criteria ensure RADIUS Attribute is set to Reply Message (18), with the Operand matches the expression, leave the value setting blank.

Ensure that the radio button for ?Show Generic Login Page? is selected.

Click on Save Changes.


Auth Servers > PINsafe >

Edit Custom Radius Rule

Name: PIN

If received Radius Response Packet ...

Response Packet Type: Access Challenge

Attribute criteria:

Radius Attribute	Operand	Value	
Reply-Message (18)	matches the expression		Add

Then take action ...

○ show **New Pin** page

○ show **Next Token** page

● show **Generic Login** page

○ show **user login page** with error message

- ○
- ○ show **Reply-Message** attribute from the Radius server to the user

○ send **Access Request** with additional attributes

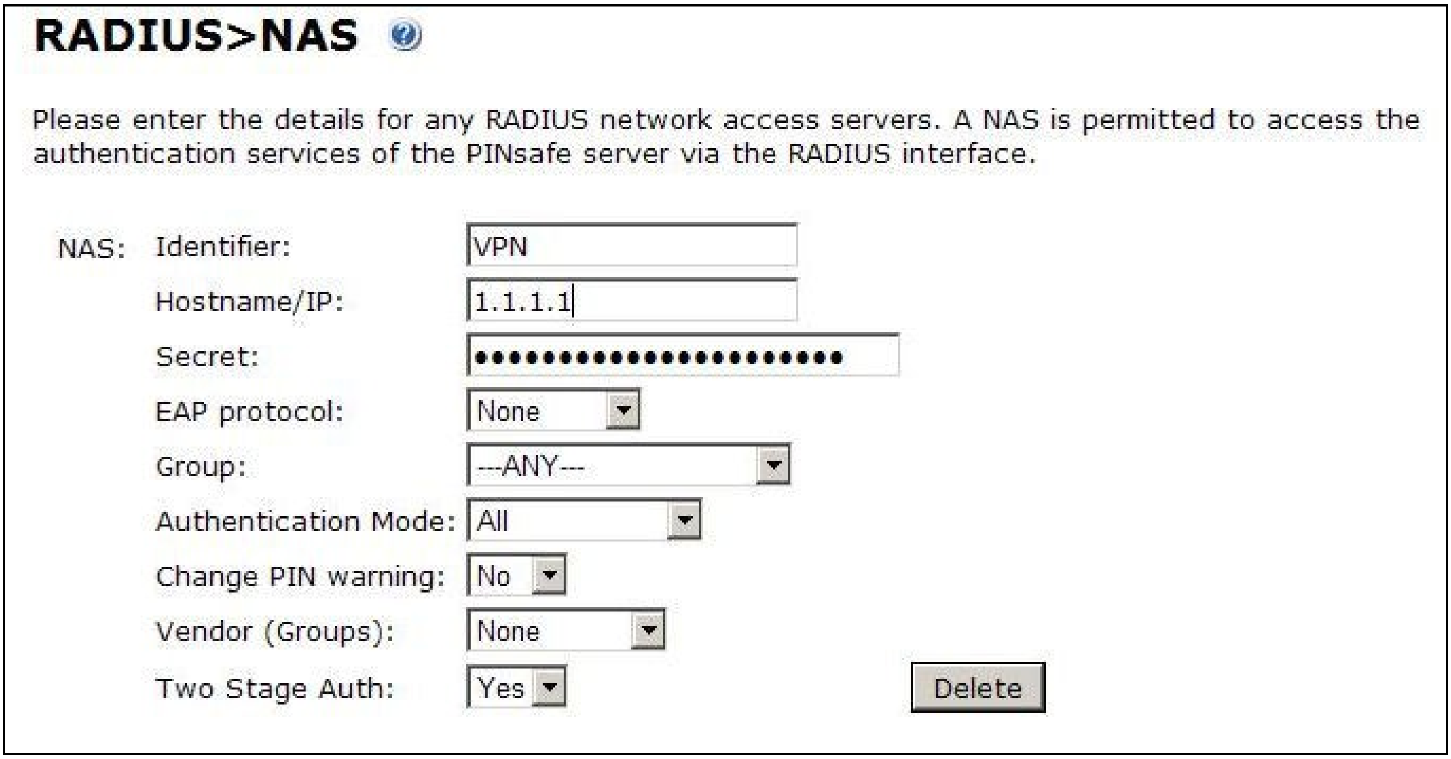
Radius Attribute	Value	
User-Name (1)		Add

Save Changes ?

Adding Challenge and response Authentication

See also: Challenge and Response How to Guide

For PINsafe 3.7 and later, on the PINsafe Administration Console server select RADIUS/NAS and ensure the Two Stage Auth is set to Yes, then click on Apply.

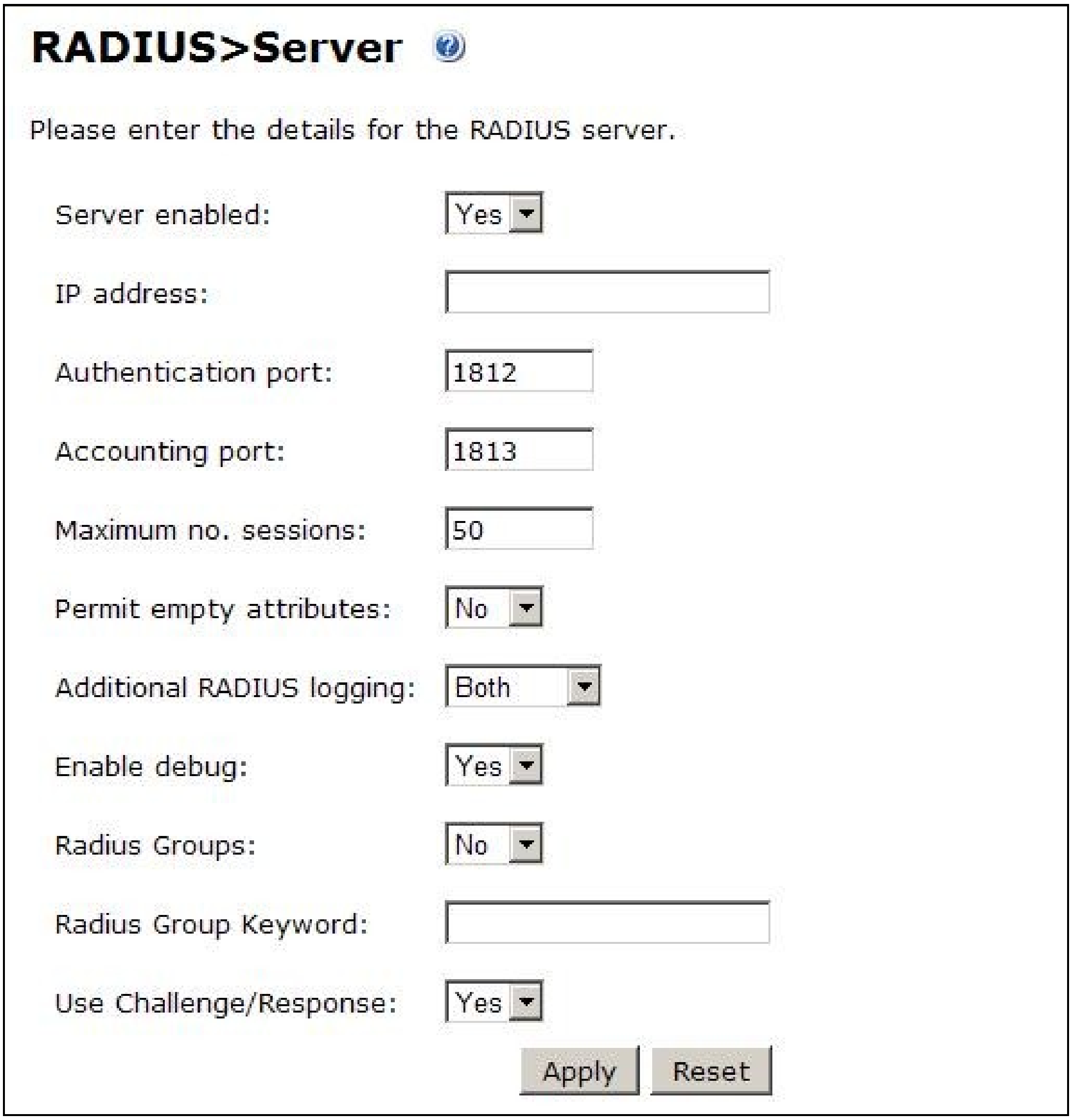


RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the PINsafe server via the RADIUS interface.

NAS:	Identifier:	VPN
	Hostname/IP:	1.1.1.1
	Secret:	••••••••••••••••••••••
	EAP protocol:	None
	Group:	---ANY---
	Authentication Mode:	All
	Change PIN warning:	No
	Vendor (Groups):	None
	Two Stage Auth:	Yes

For PINsafe 3.6 and earlier, on the PINsafe Administration Console server select RADIUS/Server and ensure the Use Challenge/Response is set to Yes, then click on Apply.

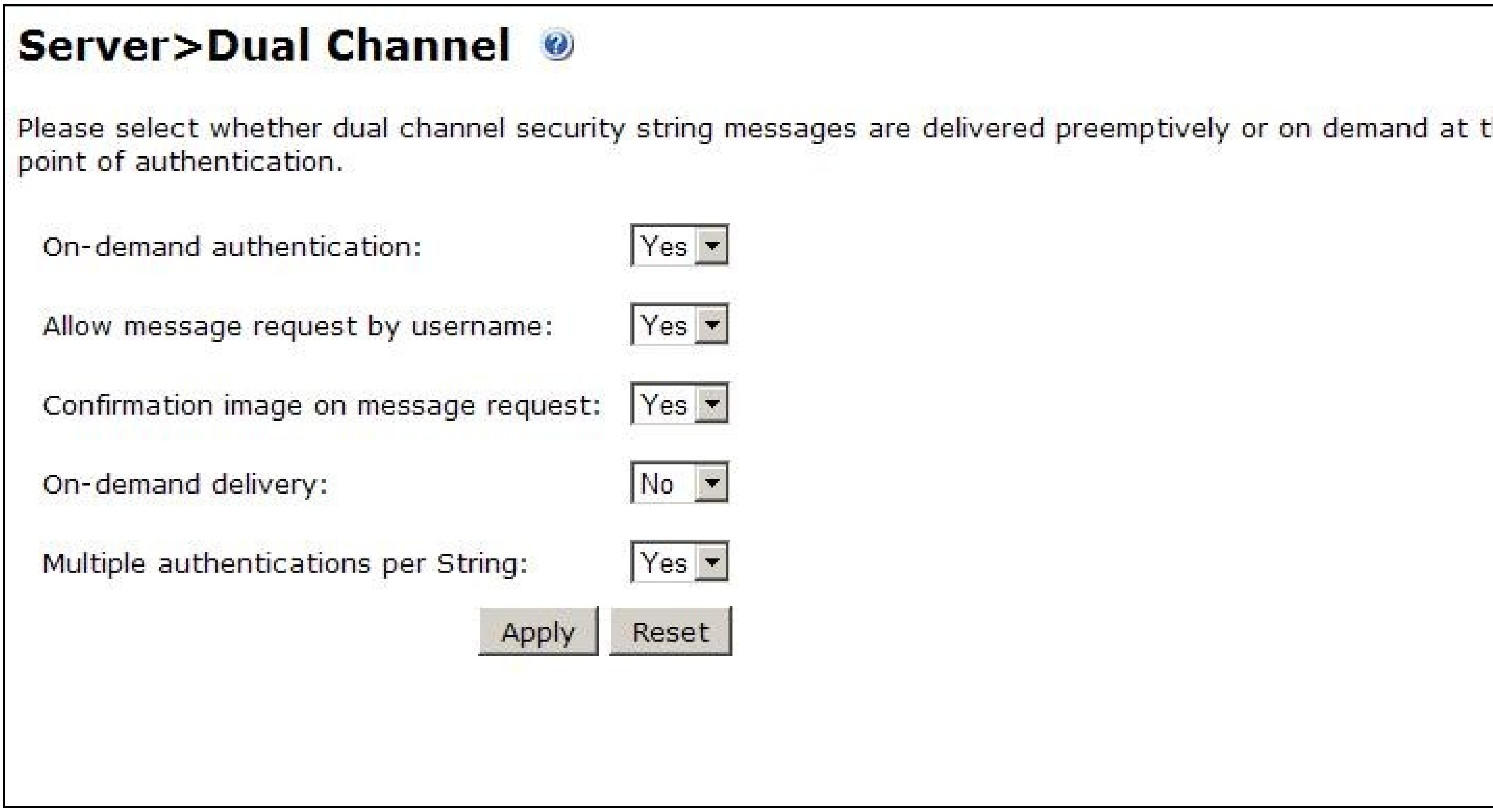


RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	No
Radius Group Keyword:	
Use Challenge/Response:	Yes

On the PINsafe Administration Console server select Server/Dual Channel. For delivery of a new security string upon entering a correct password, ensure On-Demand Authentication is set to Yes, then click on Apply.



Server>Dual Channel

Please select whether dual channel security string messages are delivered preemptively or on demand at t
point of authentication.

On-demand authentication: Yes

Allow message request by username: Yes

Confirmation image on message request: Yes

On-demand delivery: No

Multiple authentications per String: Yes

Combining Juniper and PINsafe Two Stage Authentication

Using the Juniper AD authentication is useful for single Sign On (SSO) features, so it may be of use to combine the Juniper Two Stage login with that of the PINsafe Two Stage authentication in order to send the user a security string or OTC when the AD password is entered. To configure this:

Enable Two Stage Authentication on the Juniper

Enable two Stage Authentication on the PINsafe Administration Console

Enable Check Password with Repository on the PINsafe Administration Console, See Check Password With Repository

On the Juniper select the User Realm relating to the required Authentication Realm and change the **set Password is:** to the value **Predefined as <PASSWORD>**

When an authentication is made, the AD password is used for the Juniper and the PINsafe Two Stage Authentication so it does not need to be entered twice.

Verifying the Installation

Check the PINsafe logs

Check the Juniper logs

Troubleshooting

View the users security string to ensure the correct security string is being used.

Ensure authentication is working with standard authentication.

Known Issues and Limitations

PINsafe 3.7 Beta required the use of Multiple Authentications per string to be enabled for dual/single channel located on the PINsafe Administration console under Server/Single Channel or Server/Dual Channel.

Additional Information

Juniper can also be configured for Constrained Delegation where a PINsafe One Time Code is entered and this signs the user into their AD applications without the use of an AD password in the login process. See the following documentation: http://www.juniper.net/techpubs/software/ive/6.x/6.4/

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com