Challenge and Response How to Guide

Contents

- 1 Challenge and Response Authentication
- 2 Introduction
- 3 Prerequisites
- 4 Architecture
- 5 Installation
    - 5.1 Challenge and Response Swivel 3.10 onwards
    - 5.2 Challenge and Response Swivel 3.8-3.9.x
    - 5.3 Challenge and response Swivel 3.7
    - 5.4 SMS Configuration
    - 5.5 Unknown user option
    - 5.6 Multiple Security Strings and Mobile Client
- 6 Verifying the Installation
- 7 Troubleshooting
    - 7.1 Error Messages
- 8 Known Issues and Limitations
- 9 Additional Information

Challenge and Response Authentication

Introduction

This is where a user enters a password (see Password How to Guide), the password field cannot be empty, and if this is correct the user will then be sent automatically a One Time Code for authentication by their transport (see On Demand Authentication). The benefit of Challenge and Response authentication is that the Transport delivery is password protected against malicious requests. see Also Challenge response.

Prerequisites

Swivel 3.7 onwards

Swivel 3.9.6 for Multiple Security strings and Mobile Client

Access Device which supports RADIUS Challenge and Response

Dual Channel authentication

Architecture

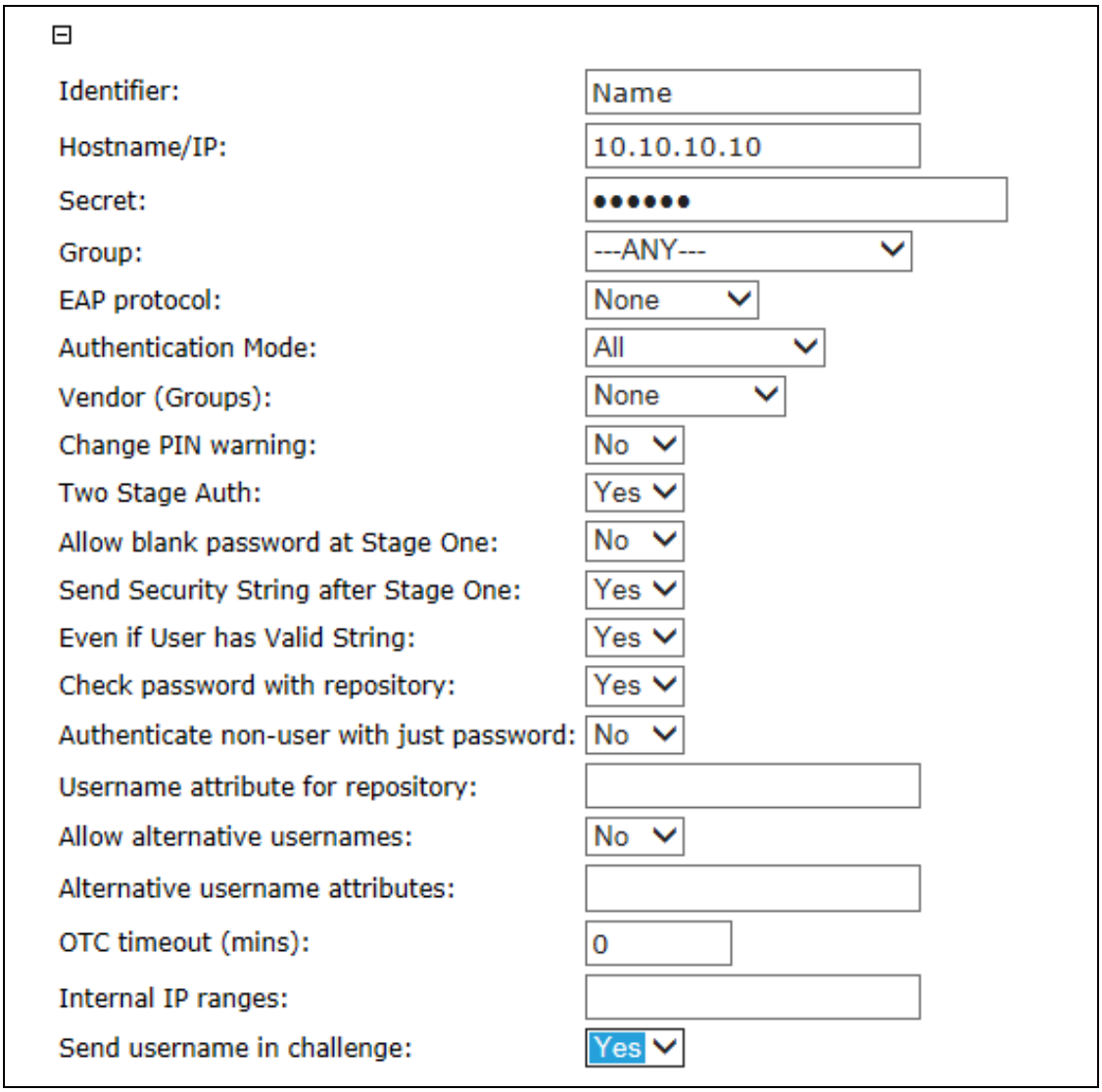
Swivel configured as a RADIUS server, when a password is successfully entered the user is sent a One Time Code by their defined transport.

Installation

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

Challenge and Response Swivel 3.10 onwards

In version 3.10 onwards, there are a number of options available for use with challenge-response:



The important option is to set Two Stage Auth to Yes, to enable Challenge-Response.

Other options which are useful for challenge-response are as follows:

- Allow blank password at Stage One - in this case, you would just enter the username in the first stage.
- Send Security String after Stage One - controls whether an on-demand message containing a security string should automatically be sent after a successful first-stage authentication.
- Even if User has Valid String - works with the previous option to suppress the on-demand message if the user already has a valid security string.
- Check password with repository - this will use the repository (e.g. Active Directory) password to authenticate at stage 1, rather than the Swivel password.
- Send username in challenge - The Challenge will be prefixed by the username, followed by a colon. Necessary when using single-channel authentication and the second-stage page does not show the username. You should check the documentation on the specific integration to decide whether or not this option is required.

There are also further, hidden options available to control which users receive dual-channel messages:

You can create a file in the configuration folder - on an appliance, this is /home/swivel/.swivel/conf - called "radius-challenges.txt". This consists of a list of Swivel groups, one per line, in the format

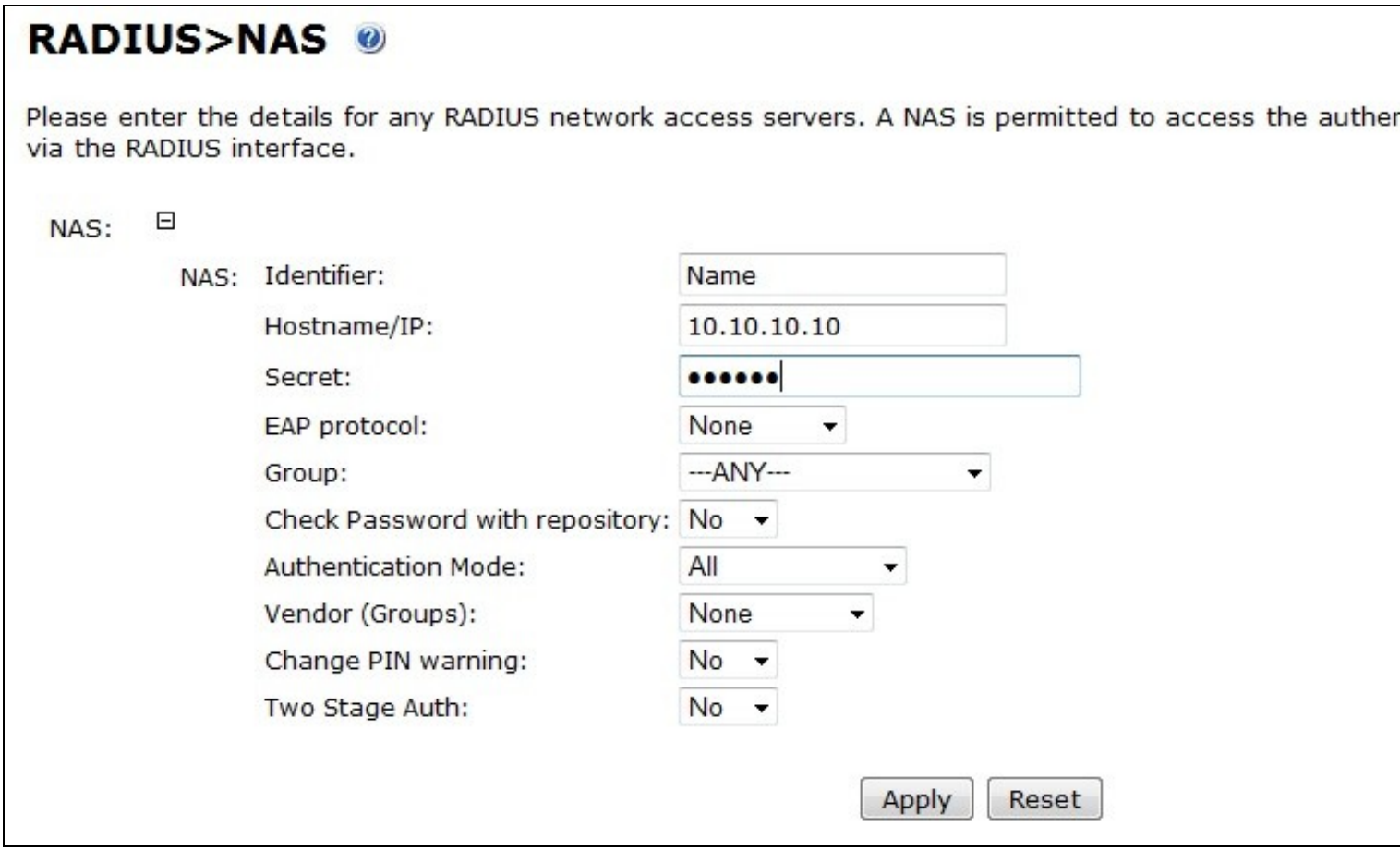
```
group-name, challenge, send
```

The first field is the name of the group. The second is a custom challenge. This allows you to override the challenge sent for certain groups. If this is missing, the default challenge ("One-Time Code") is used. The third field is either 1 or 0, indicating whether or not users in this group should be sent dual-channel messages. If this is missing, the default behaviour is used.

New behaviour for version 4.1.3: In version 4.1.3, additional options were added to radius challenges to allow more control over Push authentication. Specifically, if the challenge is "PUSH" and there is no send option, then this group will use Push authentication, irrespective of whether the NAS is configured for Push. Conversely, if the challenge is "NOPUSH" and there is no send option, this group will not use Push authentication if Push is enabled for the NAS.

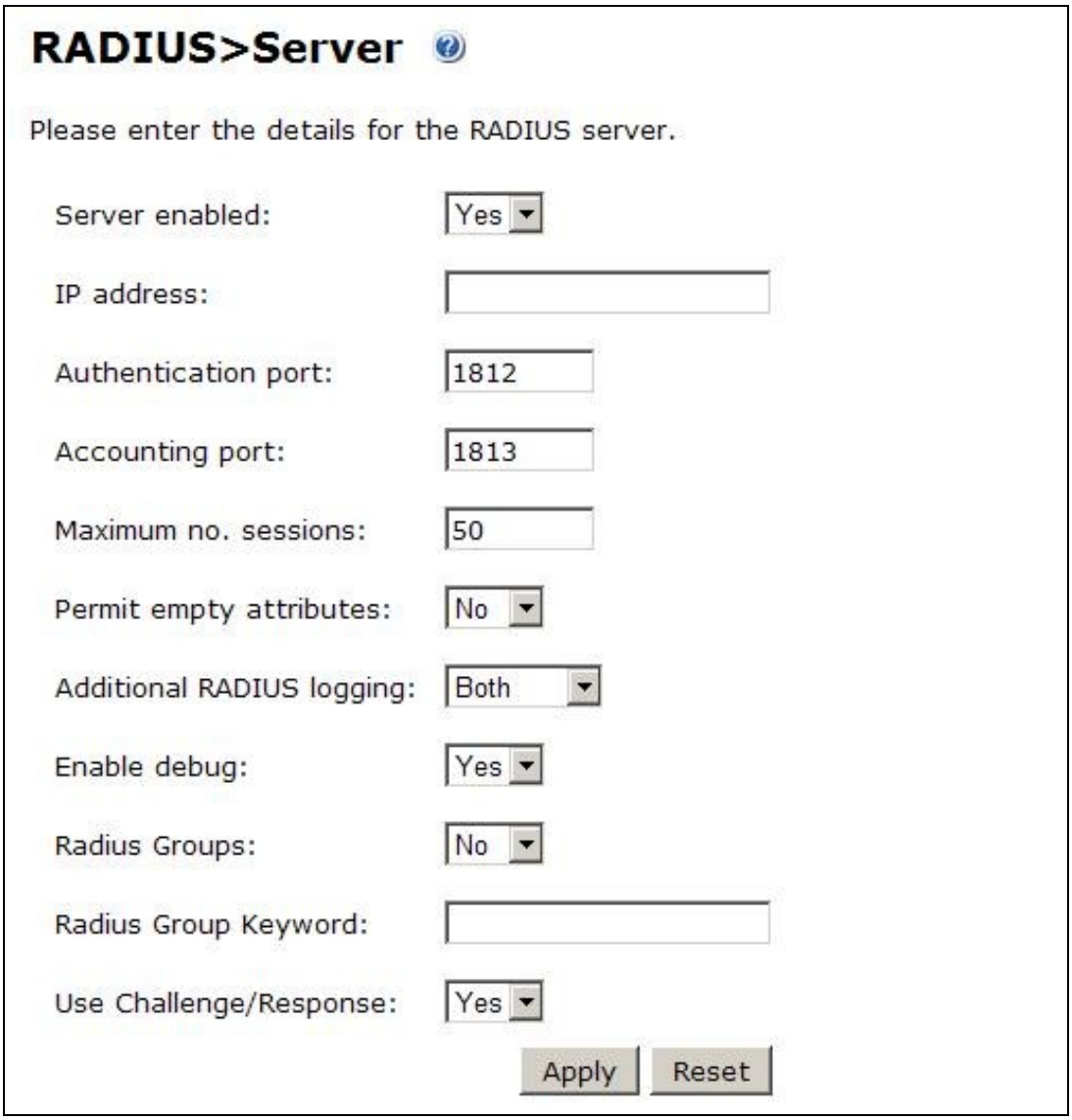
Challenge and Response Swivel 3.8-3.9.x

For Swivel 3.8 Challenge and Response Authentication is used when Two Stage Authentication is enabled. On the PINsafe Administration Console select RADIUS/NAS then set the Two Stage Auth to Yes.

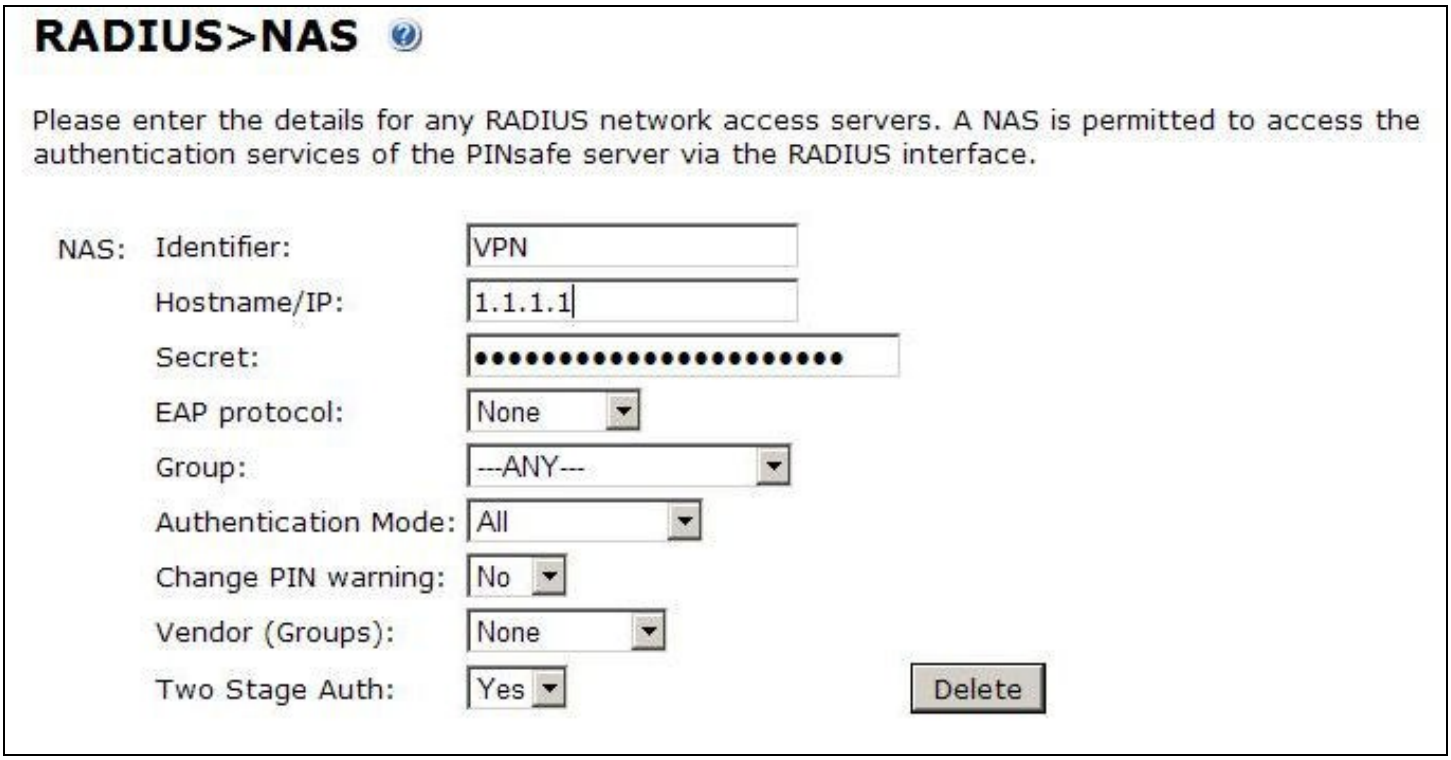


Challenge and response Swivel 3.7

On the Swivel Administration Console server select RADIUS/Server and ensure the Use Challenge/Response is set to Yes, then click on Apply



On the Swivel 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.



SMS Configuration

On the Swivel 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.



Unknown user option

Swivel 3.9.6 onwards contains the option to not use an OTC authentication if the user is knot known to Swivel.

Under Repository>Servers the following option is available:

Server to use to attempt to authenticate non-users: default None, drop down menu allows a repository to be selected for checking the user.

When a RADIUS challenge is made, if the user is not known to Swivel, it will just use the repository password and Swivel sends back a RADIUS accept if the password is correct. If the user is known to Swivel they will be challenged for an OTC.

Multiple Security Strings and Mobile Client

These are supported in Swivel version 3.9.6 for use with Two Stage Authentication.

To use this feature set **Send Security String after Stage One:** to No

Verifying the Installation

Check the Swivel logs

Check the Access Device logs

Troubleshooting

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

Ensure authentication is working with standard authentication.

If the second stage is failing try again with the repository password. If the password succeeds in the second stage and then results in another Access Challenge then the RADIUS Client may not be returning the correct **state Attribute**. This Attribute is available to be sent by the server to the client in an Access-Challenge and MUST be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. The below shows the Swivel log where the state attribute is not being returned.

```
RADIUS: <74> Access-Challenge(11) LEN=46 127.0.0.1:64214 Access-Request by graham resulted in Access-Challenge.

RADIUS: <73> Access-Challenge(11) LEN=46 127.0.0.1:64213 Access-Request by graham resulted in Access-Challenge.

RADIUS: <72> Access-Challenge(11) LEN=46 127.0.0.1:52245 Access-Request by graham resulted in Access-Challenge.
```

NTRadPing 1.5 does not support Challenge and Response for Two Stage Authentication.

Error Messages

RADIUS: <0> Access-Request(1) LEN=64 x.x.x.x:1265 Access-Request by username Failed: AccessRejectException: Two Stage Password Fail

x.x.x.x Identifier:Failed to get LDAP context for username@domain

The check password with repository is failing for the first stage of two stage authentication. This could be due to an incorrect password being entered or not recognized. On the Swivel Administration console when using AD try setting the AD server settings username to the UPN name.

Known Issues and Limitations

Additional Information

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