# Cisco SA 520

## Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
    - 5.1 Configuring the RADIUS server
    - 5.2 Setting up PINsafe Dual Channel Transports
    - 5.3 Cisco SA 520 Configuration
    - 5.4 Testing
    - 5.5 Additional Configuration Options
    - 5.6 Troubleshooting
    - 5.7 Known Issues and Limitations
    - 5.8 Additional Information

## Introduction

This document describes steps to configure a Cisco SA 520 with PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility.

For the Cisco IPSEC client PINsafe integration see Cisco IPSEC Client Integration

Many Thanks to Brian Norrie of NCI Systems in contributing to this article.

## Prerequisites

Cisco SA 520

Cisco documentation

PINsafe 3.x, 3.5 for RADIUS groups

## Baseline

Cisco SA 520 firmware version 2.1.51

PINsafe 3.8

PAP Authentication was tested in this setup

## Architecture

The Cisco 520 makes authentication requests against the PINsafe server by RADIUS.

# Swivel Configuration

## Configuring the RADIUS server

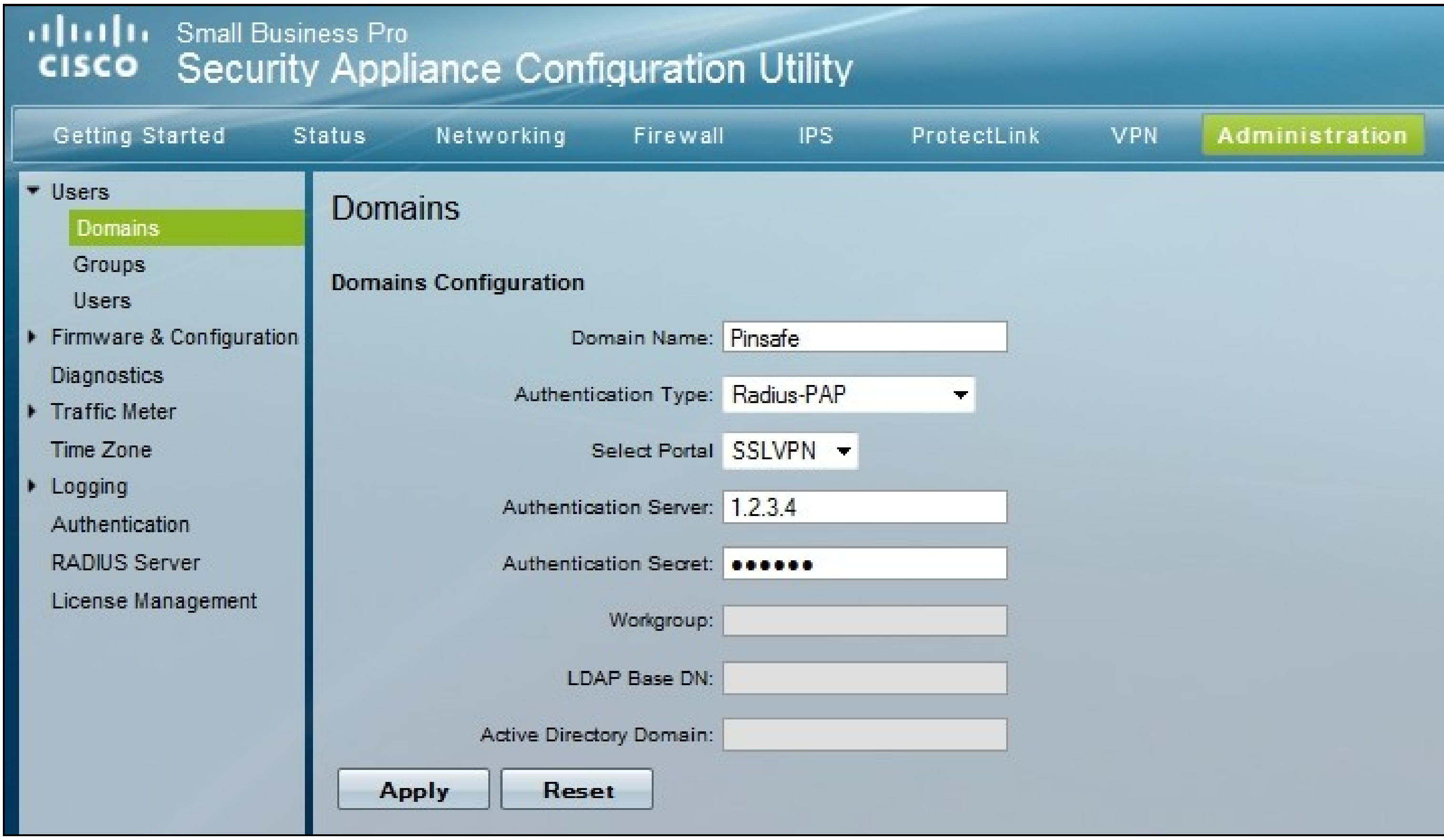
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

## Setting up PINsafe Dual Channel Transports

See Transport Configuration

## Cisco SA 520 Configuration

On the Cisco SA 520 Administration console select the Administration tab then users and domains. Click on Add, and enter the PINsafe RADIUS server authentication details for the portal.



Domains

Domains Configuration

Domain Name: Pinsafe

Authentication Type: Radius-PAP

Select Portal SSLVPN

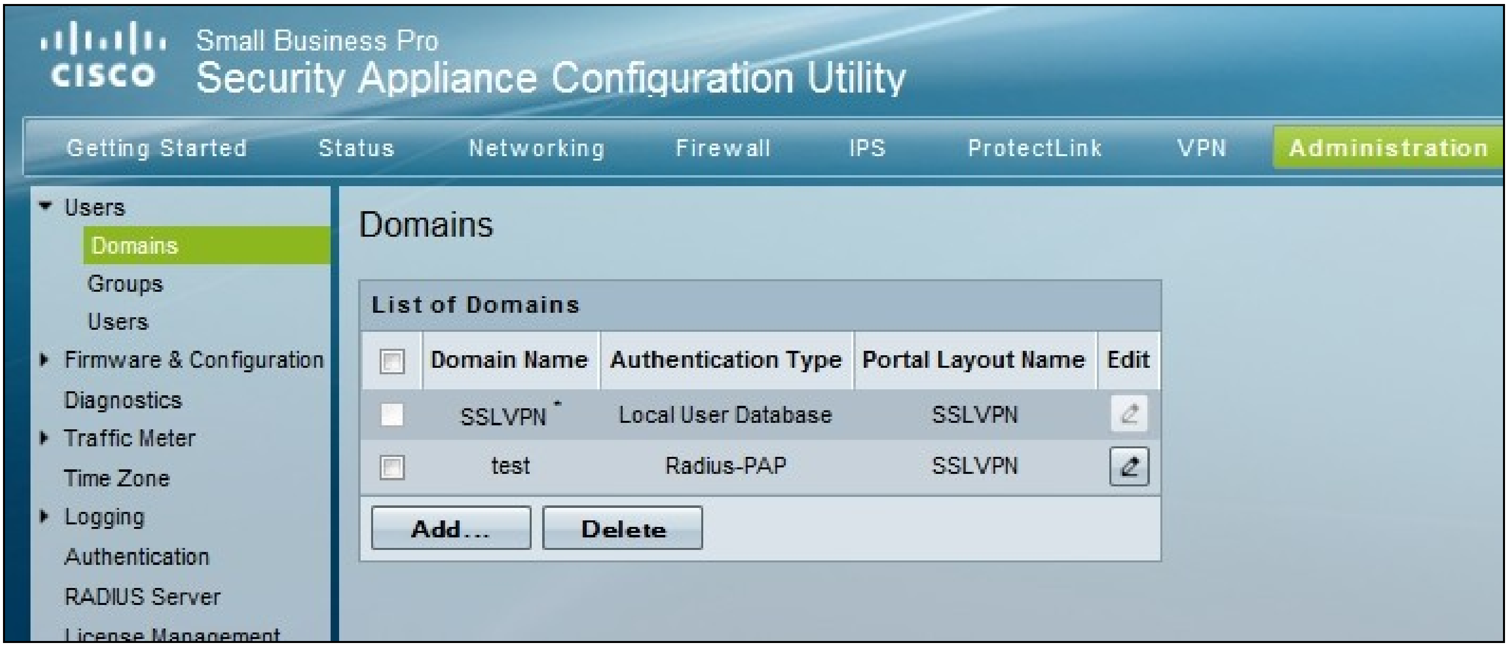
Authentication Server: 1.2.3.4

Authentication Secret: ●●●●●●

Workgroup:

LDAP Base DN:

Active Directory Domain:



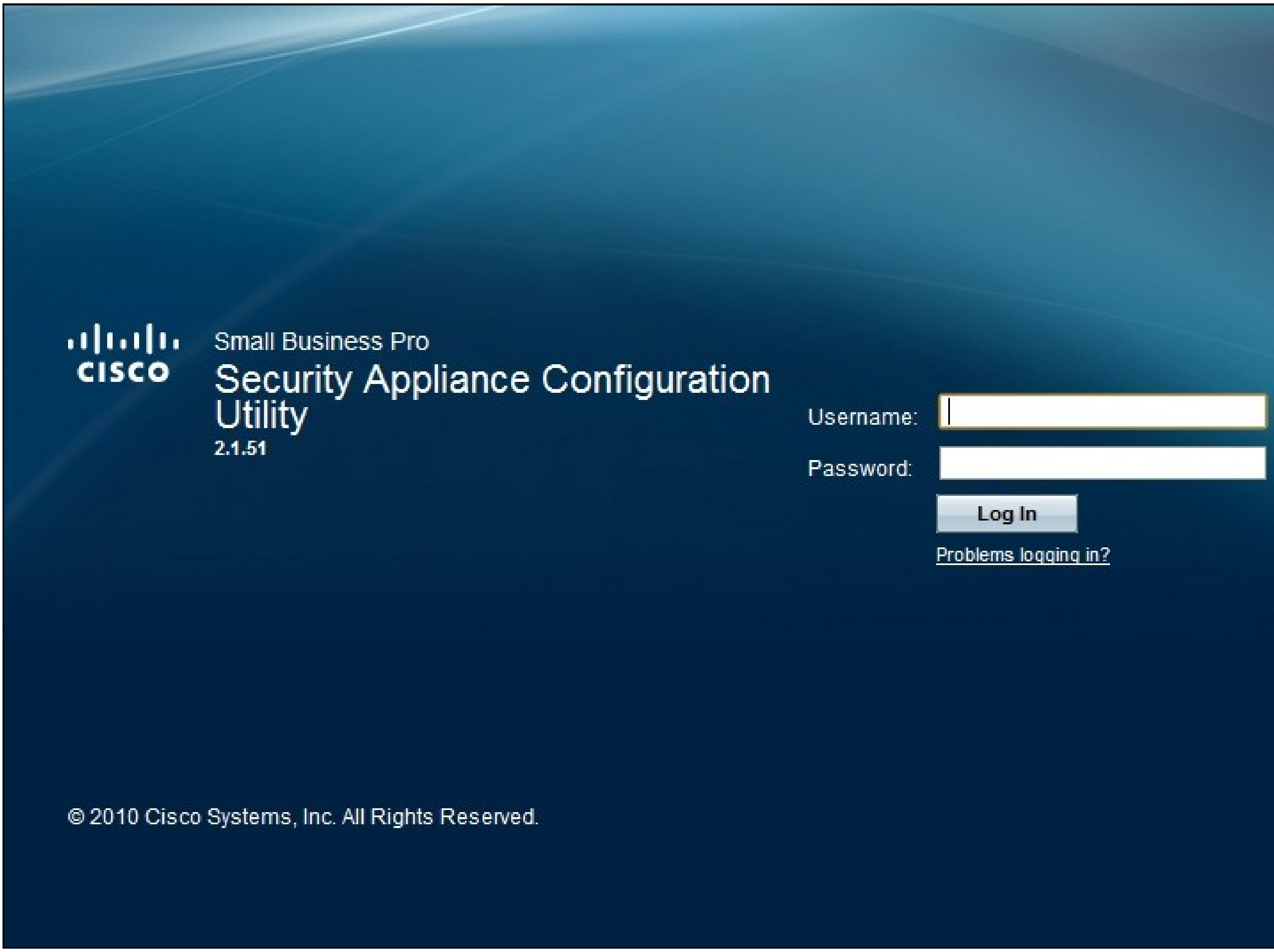
Domains

List of Domains

| □ | Domain Name | Authentication Type | Portal Layout Name | Edit |
|---|---|---|---|---|
| □ | SSLVPN * | Local User Database | SSLVPN | ✎ |
| □ | test | Radius-PAP | SSLVPN | ✎ |

## Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. You will need to enter your password followed immediately by the one time code into the Password field.


cisco
Small Business Pro
Security Appliance Configuration Utility
2.1.51
Username:
Password:
Log In
Problems logging in?
© 2010 Cisco Systems, Inc. All Rights Reserved.

## Additional Configuration Options

## Troubleshooting

Check the PINsafe logs for RADIUS requests.

## Known Issues and Limitations

Dual Channel authentication and Taskbar only

## Additional Information

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