AppGate Security Server

Contents

Introduction

This document describes steps to configure a AppGate Security Server from Cryptozone with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page.

Prerequisites

AppGate Security Server Appliance

AppGate documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

Login Page customisation prerequisites

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, and security string number, **for external access this is usually through a NAT**.

Baseline

AppGate Security Server Appliance

Swivel 3.8

Architecture

The AppGate Security Server makes authentication requests against the Swivel server by RADIUS.

The client makes TURing requests against the Swivel server using HTTP/HTTPS

Swivel Configuration

Configuring the RADIUS server

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

Enabling Session creation with username

To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

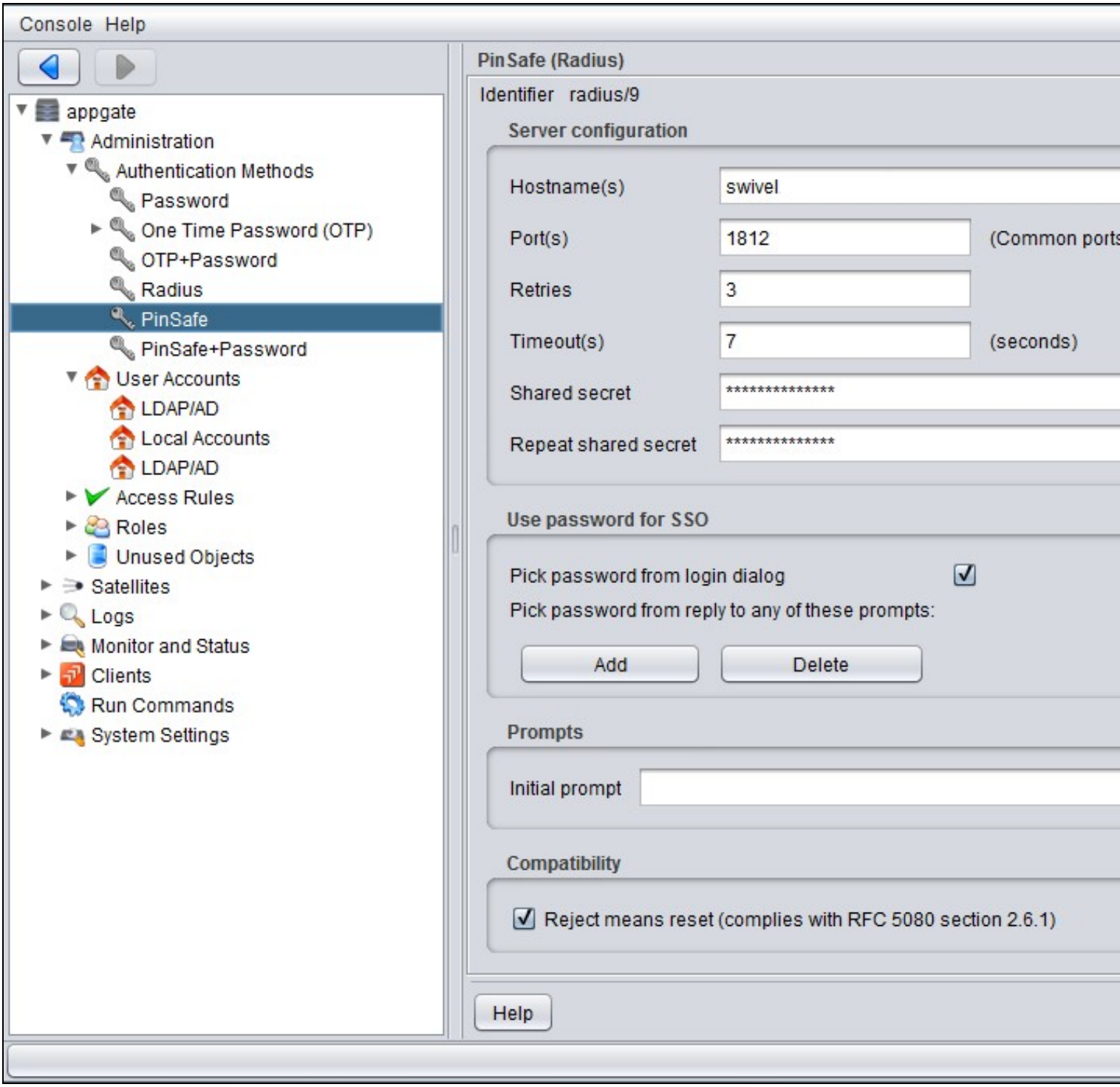
Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

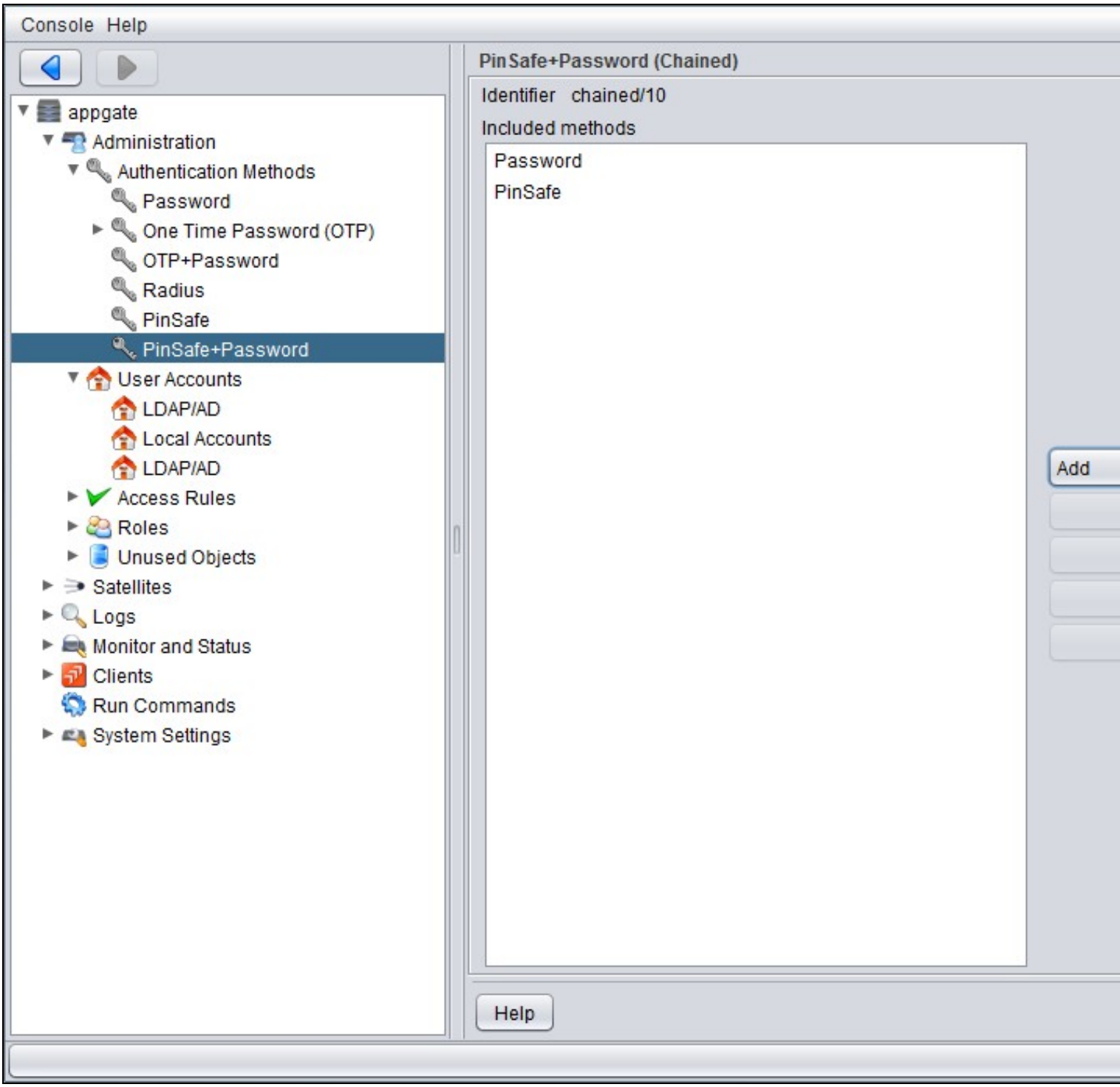
AppGate Security Server Configuration

Adding a Swivel RADIUS server

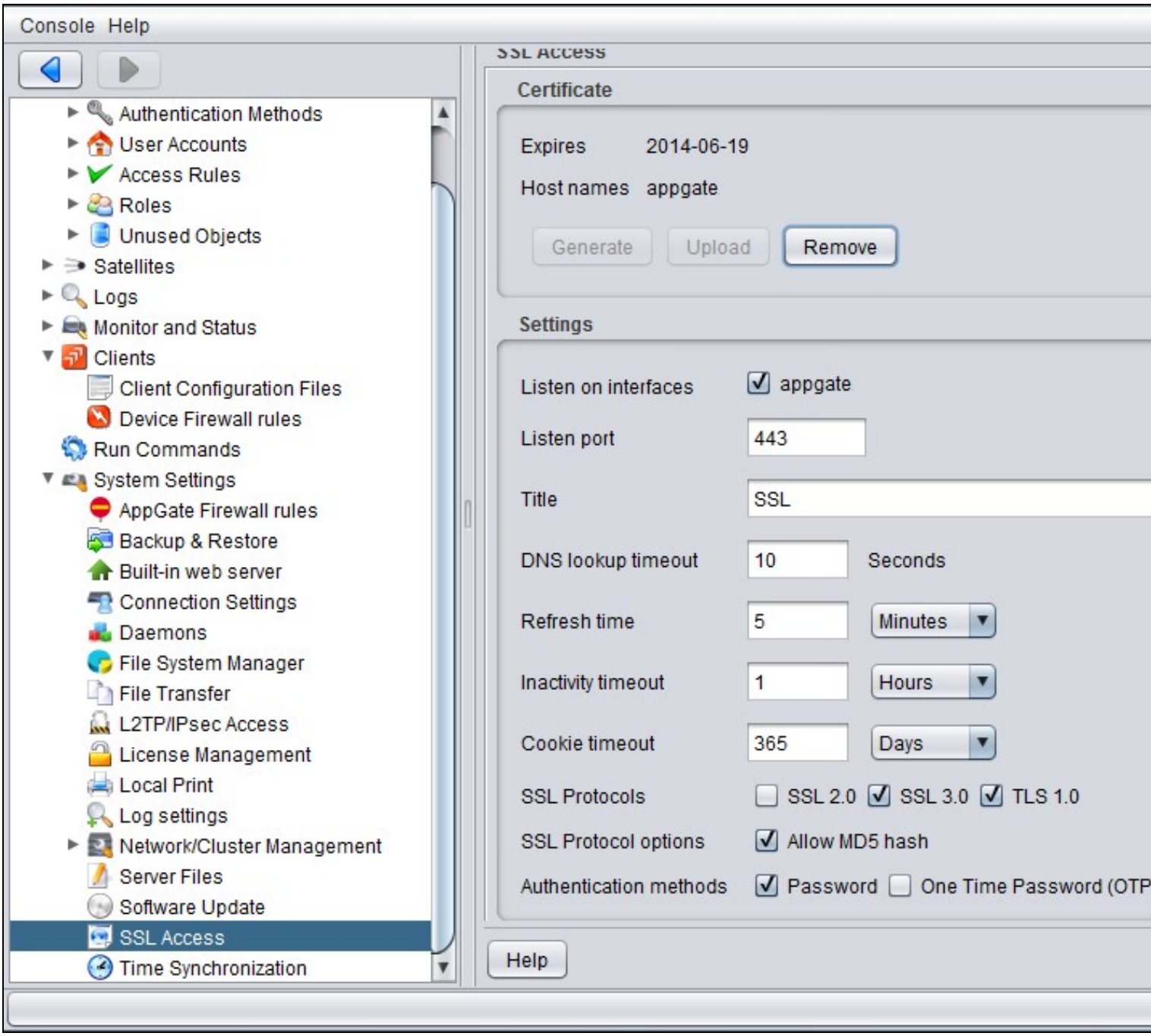
On the AppGate Security Server select Administration/Authentication Methods then Add Authentication Method.



It is recommended to use a password in combination with the OTC and this can be done by using a chained password.



On the AppGate Security Server select Administration/System Settings/SSL Access then select the required Authentication Methods allowed.



Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

Optional: Login Page Customisation

On the AppGate Security Server select Administration/User Accounts and for the required access account type ensure that RADIUS authentication is selecetd under the Authentication tab.

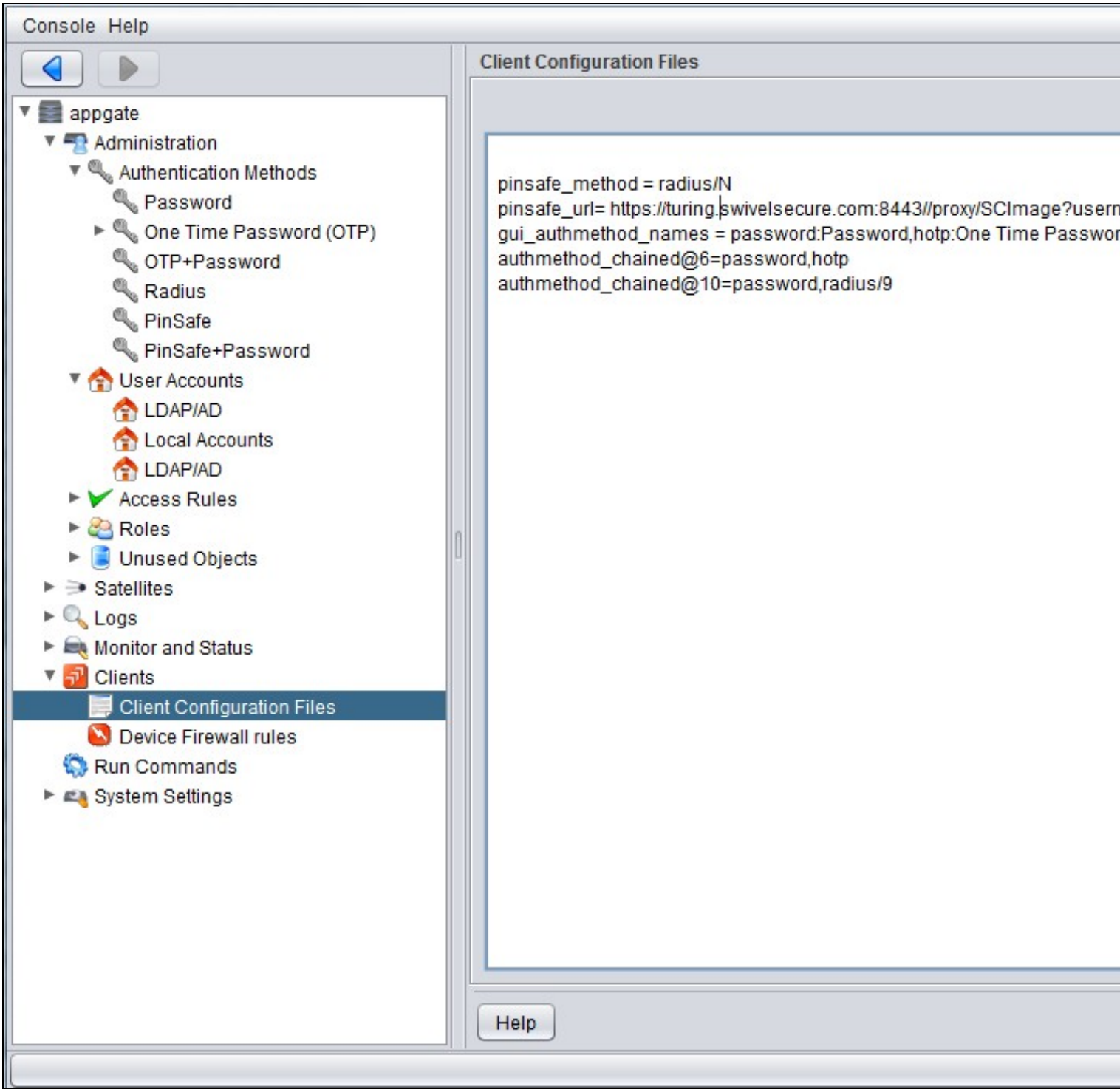
On the AppGate Security Server select Administration/Clients then Client Configuration Files and add the following lines:

pinsafe_method = radius/N

pinsafe_URL = http://server:port//pinsafe/SCImage?username=%u

where server is the Swivel sever public NAT and port the port to the Swivel server, usually 443 for a Swivel appliance. For further informationn refer to

the AppGate Security Server documentation under RADIUS/Pinsafe.



Testing

Additional Configuration Options

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Known Issues and Limitations

None

Additional Information

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