

AppGate Security Server

Contents

- 1 Introduction
- 2 Prerequisites
 - ◆ 2.1 Login Page customisation prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
 - ◆ 5.1 Configuring the RADIUS server
 - ◇ 5.1.1 Enabling Session creation with username
 - ◆ 5.2 Setting up Swivel Dual Channel Transports
- 6 AppGate Security Server Configuration
 - ◆ 6.1 Adding a Swivel RADIUS server
 - ◆ 6.2 Test the RADIUS authentication
 - ◆ 6.3 Optional: Login Page Customisation
- 7 Testing
- 8 Additional Configuration Options
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

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.

The screenshot shows the AppGate Security Server configuration interface. On the left is a navigation tree with the following structure:

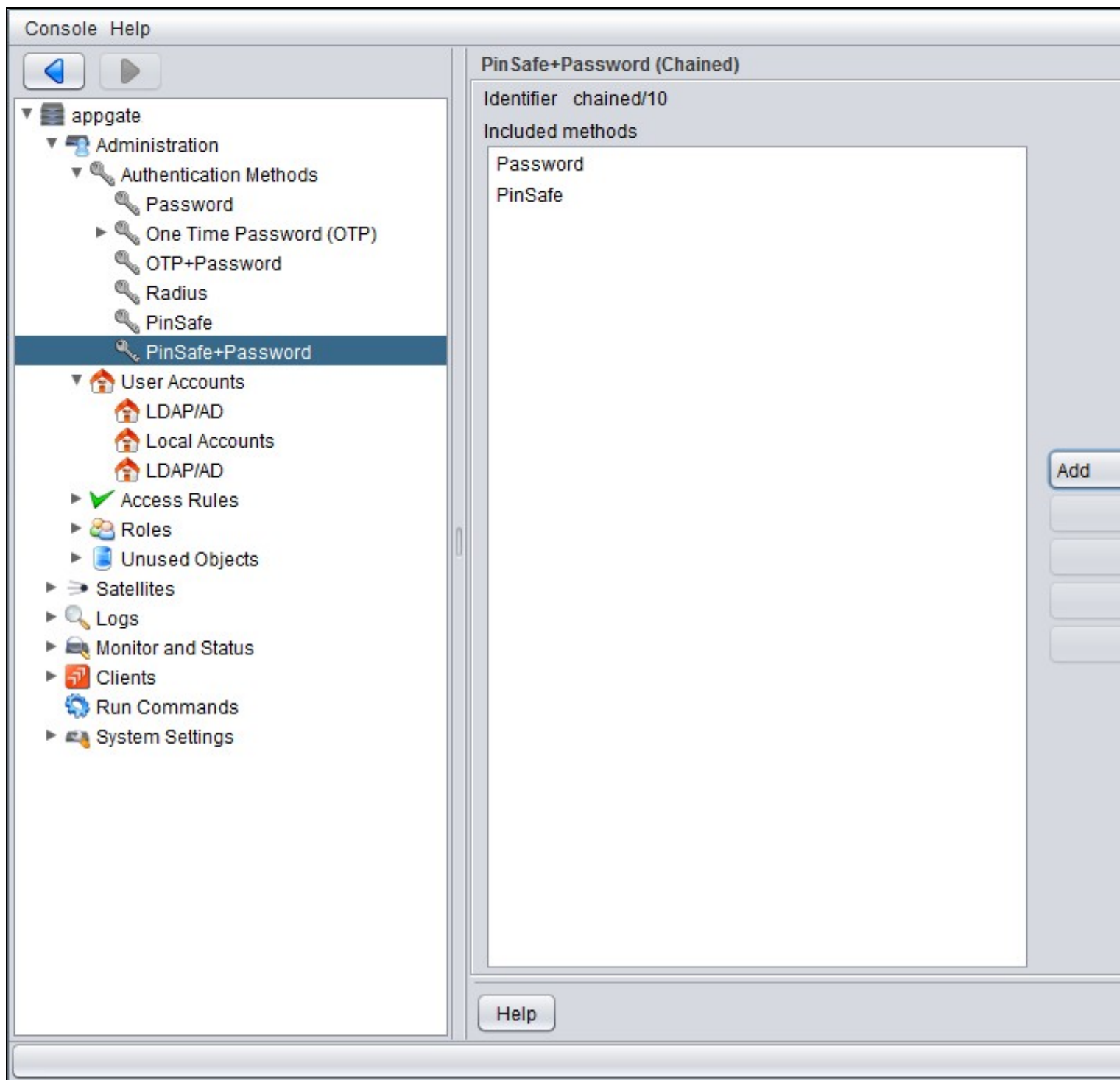
- ▼ appgate
 - ▼ Administration
 - ▼ Authentication Methods
 - ▼ Password
 - ▶ One Time Password (OTP)
 - ▼ OTP+Password
 - ▼ Radius
 - ▼ PinSafe**
 - ▼ PinSafe+Password
 - ▼ User Accounts
 - ▼ LDAP/AD
 - ▼ Local Accounts
 - ▼ LDAP/AD
 - ▶ Access Rules
 - ▶ Roles
 - ▶ Unused Objects
 - ▶ Satellites
 - ▶ Logs
 - ▶ Monitor and Status
 - ▶ Clients
 - ▶ Run Commands
 - ▶ System Settings

The main configuration area on the right is titled "PinSafe (Radius)". It contains the following sections:

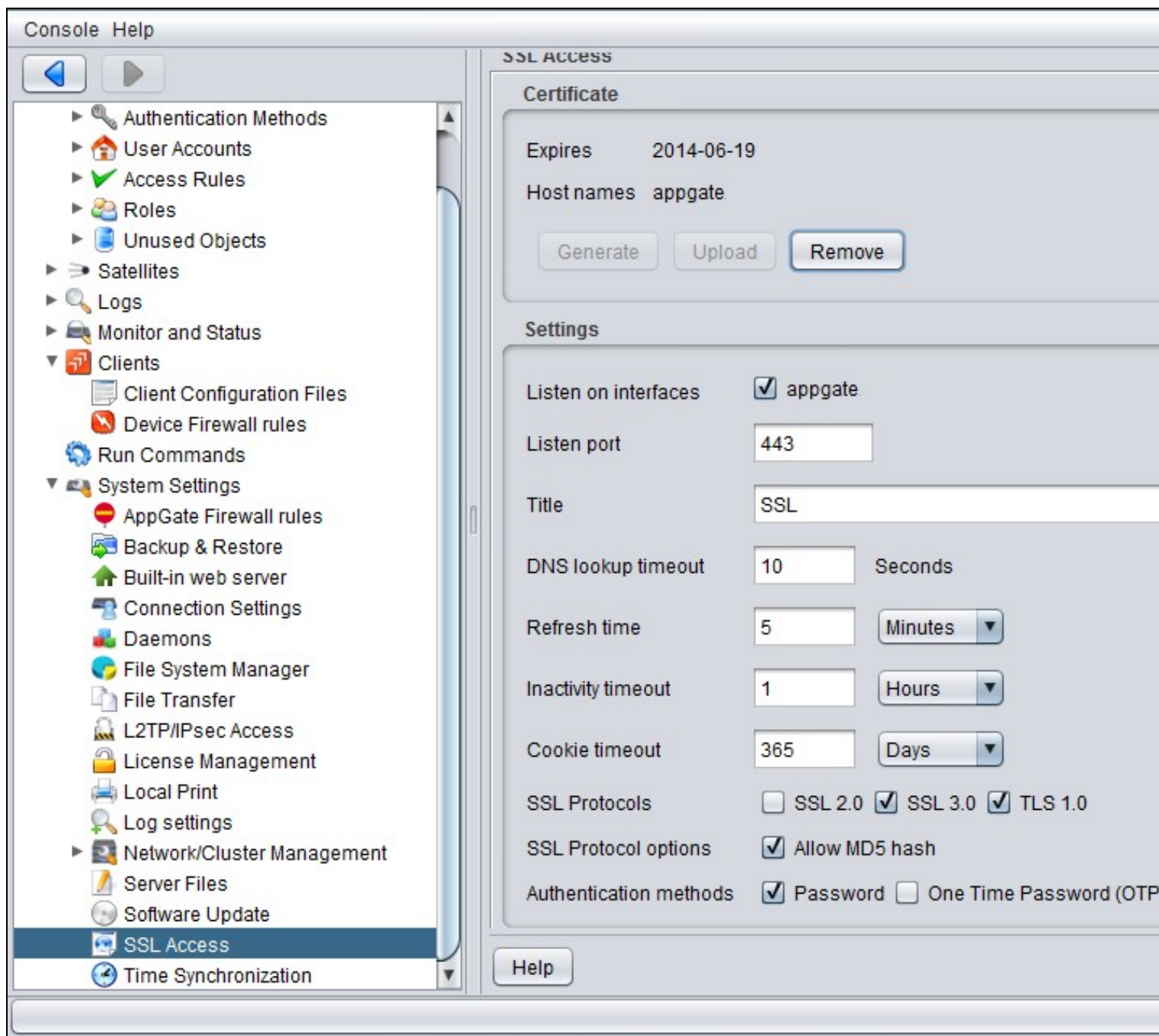
- Identifier** radius/9
- Server configuration**
 - Hostname(s): swivel
 - Port(s): 1812 (Common ports)
 - Retries: 3
 - Timeout(s): 7 (seconds)
 - Shared secret: *****
 - Repeat shared secret: *****
- Use password for SSO**
 - Pick password from login dialog: ☒
 - Pick password from reply to any of these prompts:
 - Add
 - Delete
- Prompts**
 - Initial prompt:
- Compatibility**
 - ☒ Reject means reset (complies with RFC 5080 section 2.6.1)

A "Help" button is located at the bottom of the configuration area.

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 OTP for the user. At the SSL VPN login enter the required OTP. 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

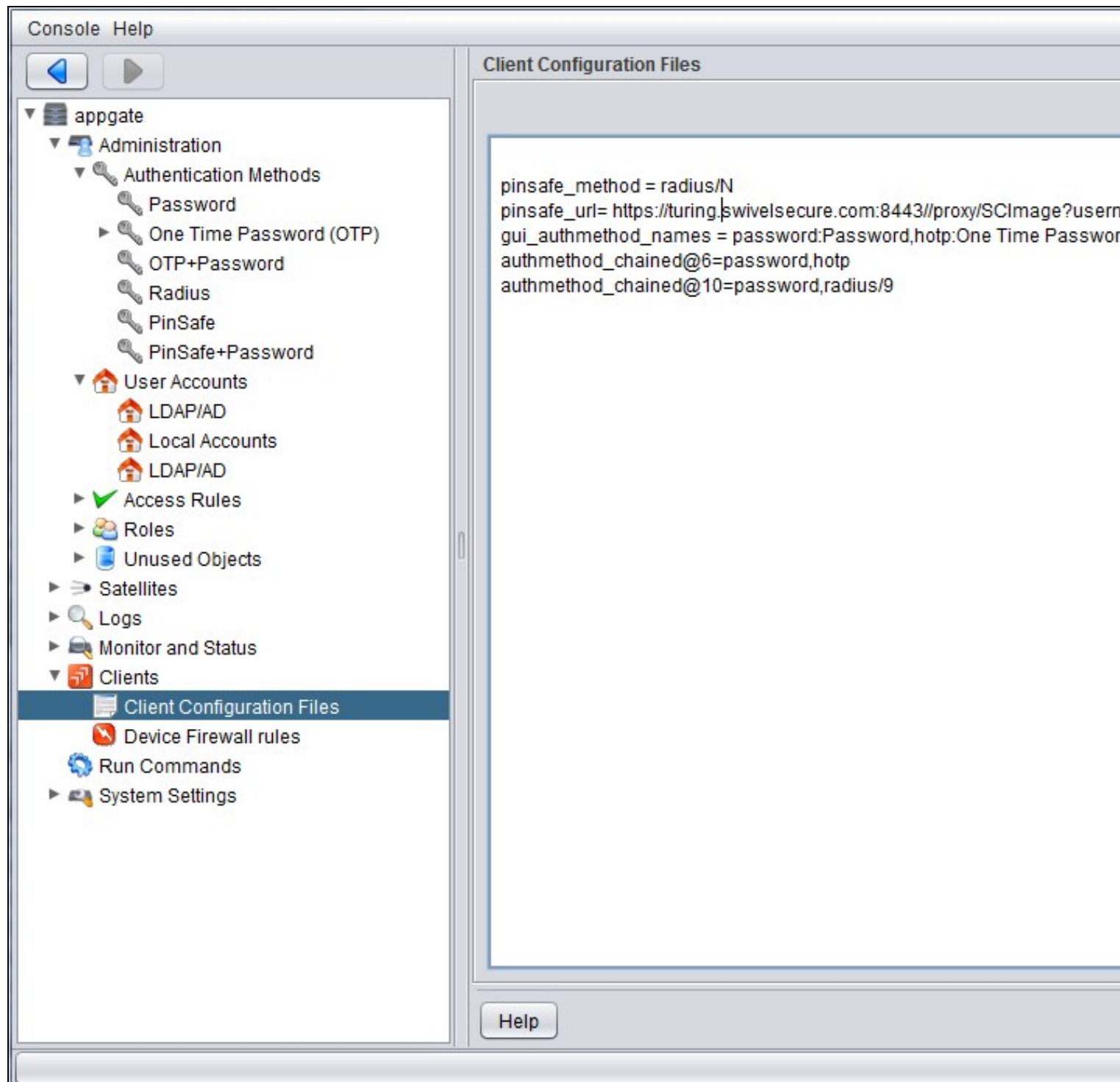
On the AppGate Security Server select Administration/User Accounts and for the required access account type ensure that RADIUS authentication is selected under the Authentication tab.

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



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