Stonesoft Integration

Contents

Introduction

This document describes steps to configure a Stonesoft Firewall SSL VPN with Swivel as the authentication server.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page. Depending on your needs, you can modify the default customization object or create a new customization object. There are many ways to configure it to work with Swivel.

To use the Single Channel Image such as the TURing Image and PINpad, the Swivel server must be made accessible. **The client requests the images from the Swivel server, and is usually configured using a NAT** (Network Address Translation), often with a proxy server. The Swivel appliance is configured with a proxy port to allow an additional layer of protection.

Prerequisites

Stonesoft Firewall

Swivel 3.x

Modified login page for TURing

Modified login page for PINpad

Baseline

Stonesoft 4.9.9|1050

Swivel 3.9

Architecture

Stonesoft makes authentication requests against the Swivel server by RADIUS.

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

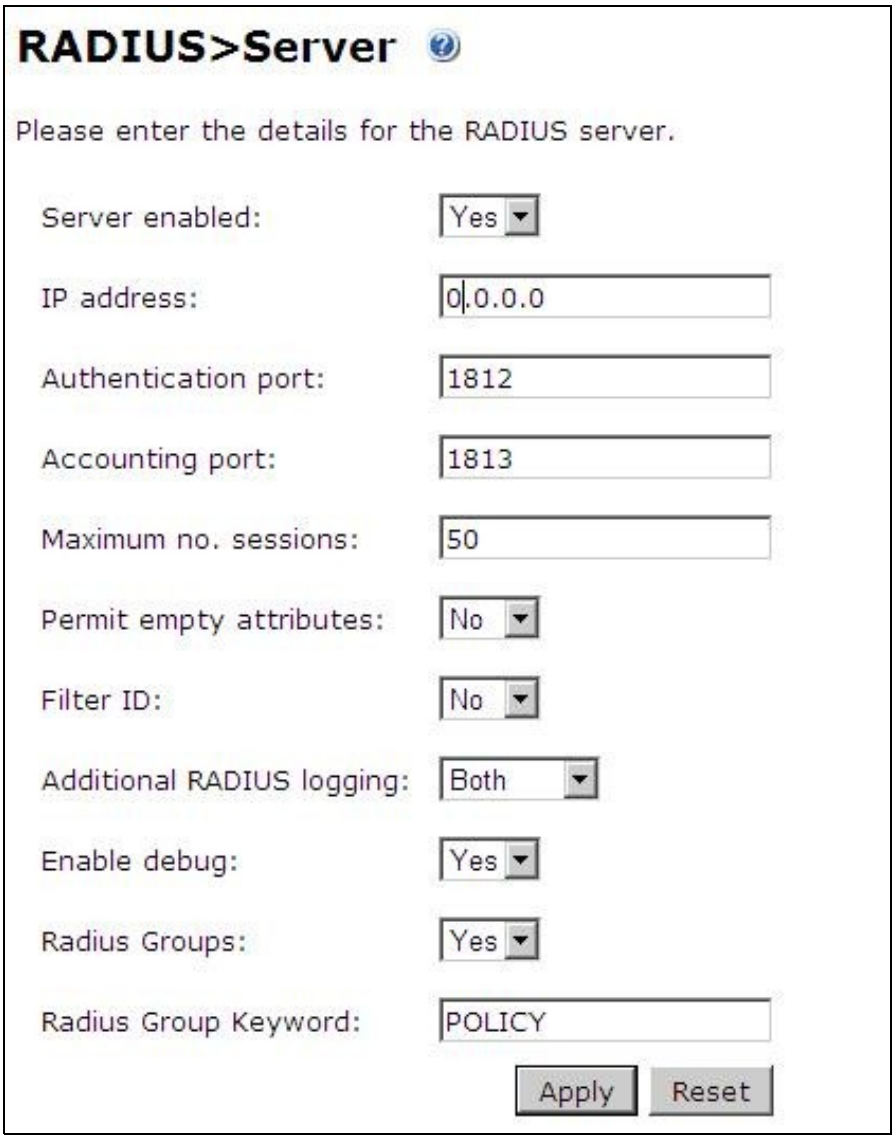
Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank (or use 0.0.0.0) to allow RADIUS requests on any interface.

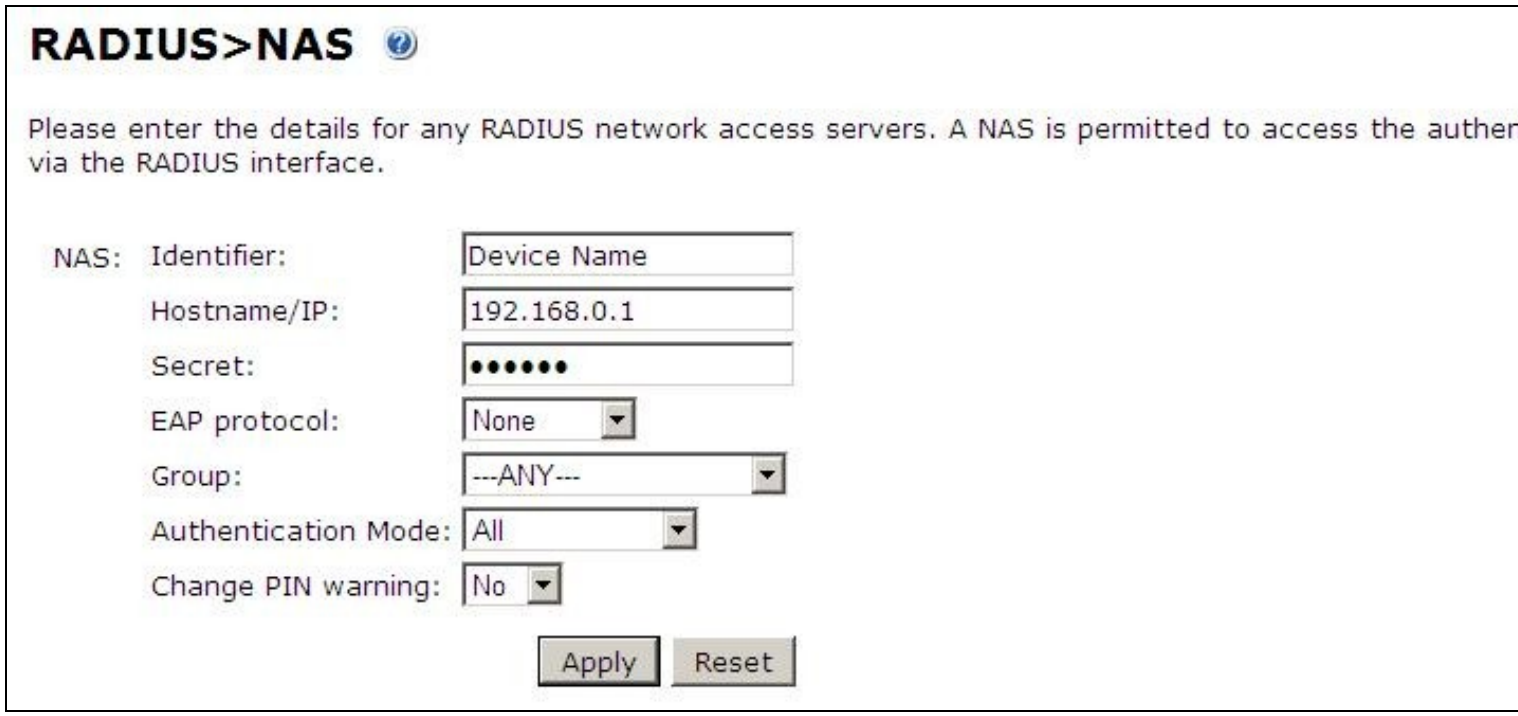
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances



Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the Swivel server and VPN RADIUS configuration.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel server can be configured to return an image containing a TURing image by presenting the username via the XML API or the SCImage servlet.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

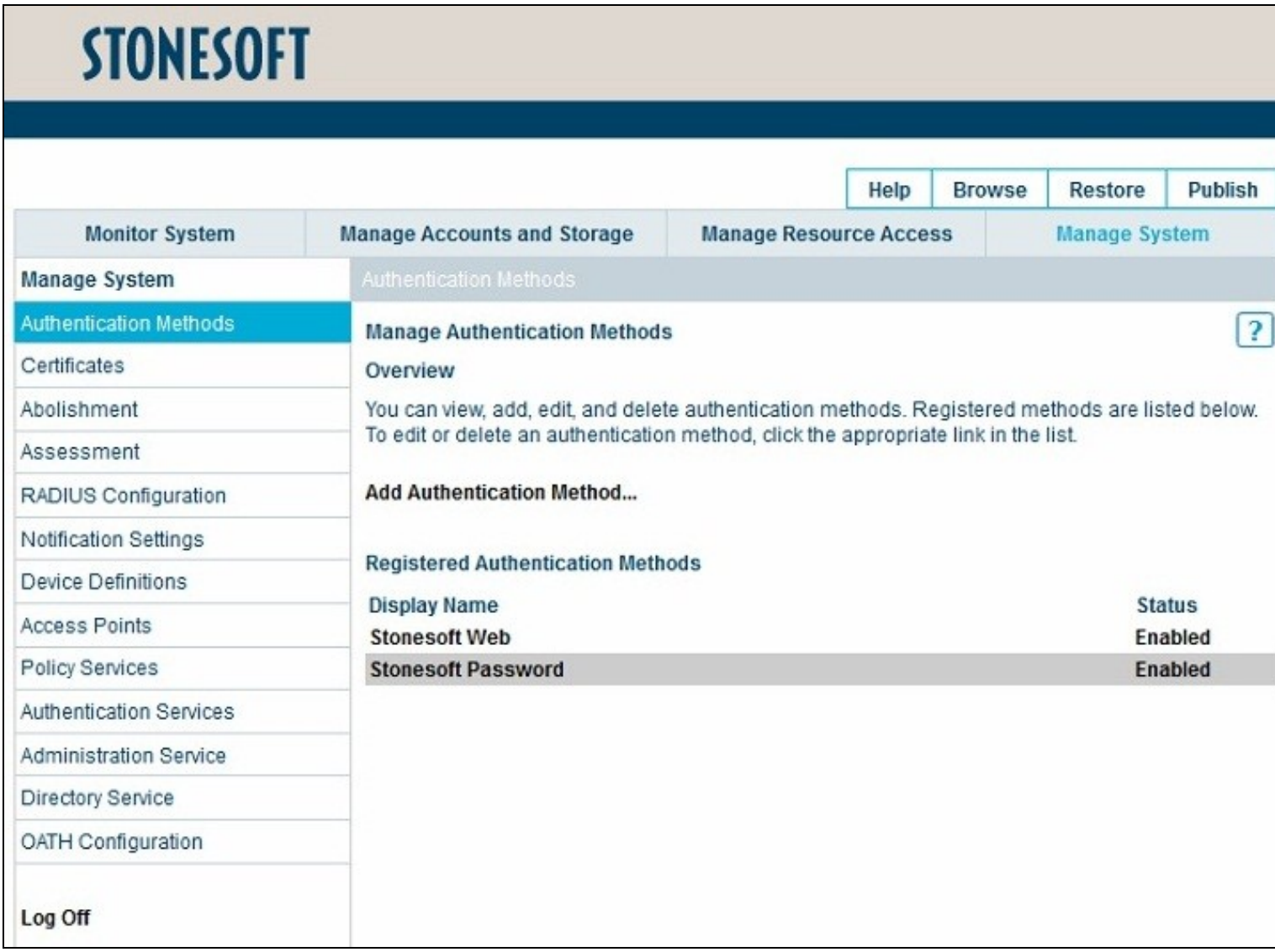
https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installation

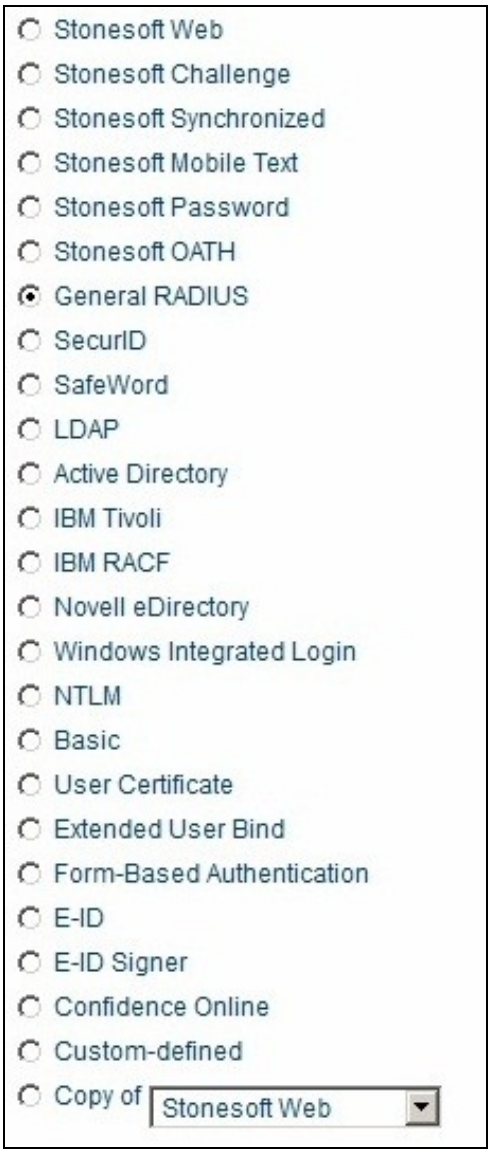
Stonesoft Configuration

Create a Radius Authentication Method

On the Stonesoft management console select the *Manage System* tab and then *Authentication Methods*, select *Add Authentication Method...*



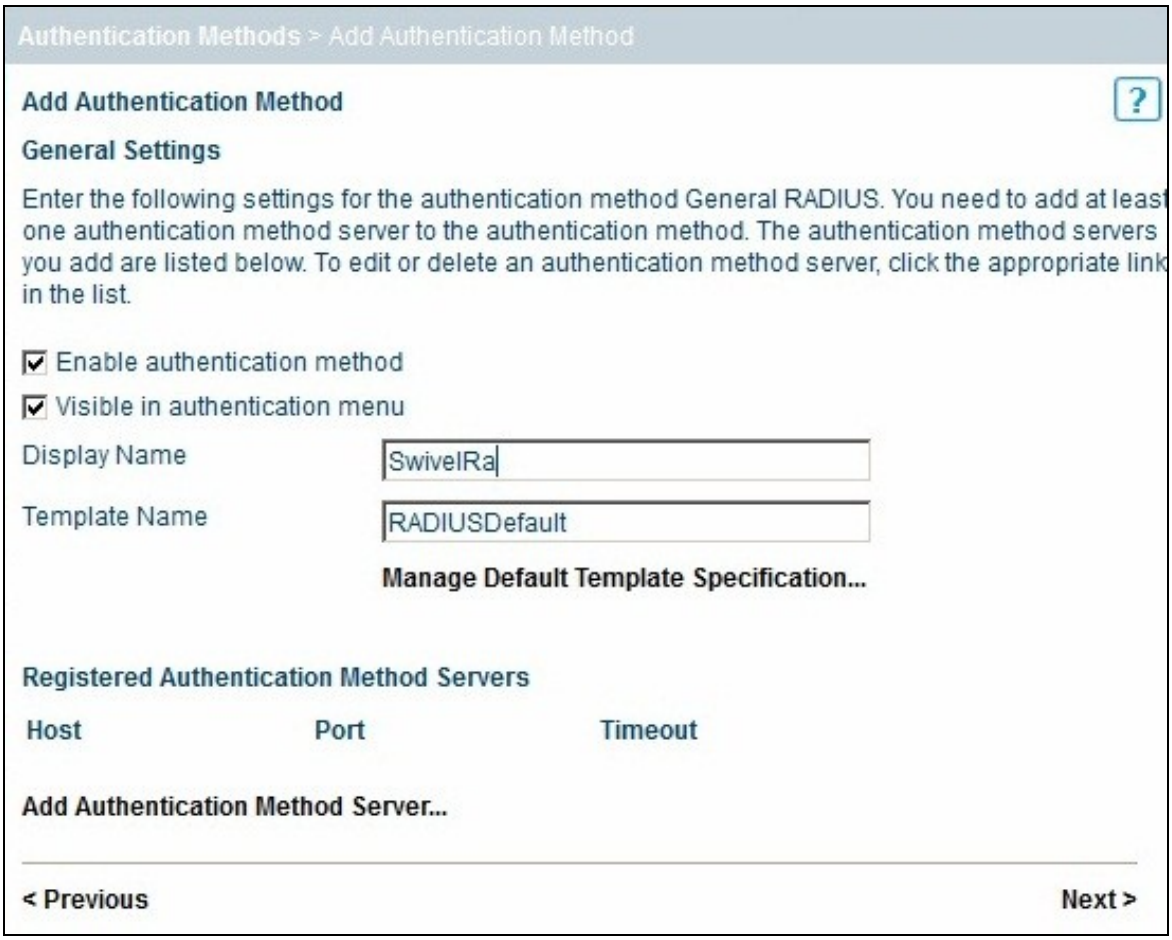
Select the *General RADIUS* authentication method



Ensure the following are checked:

- *Enable authentication method*
- *Visible in authentication menu*

Enter a Display Name, then click on Next.



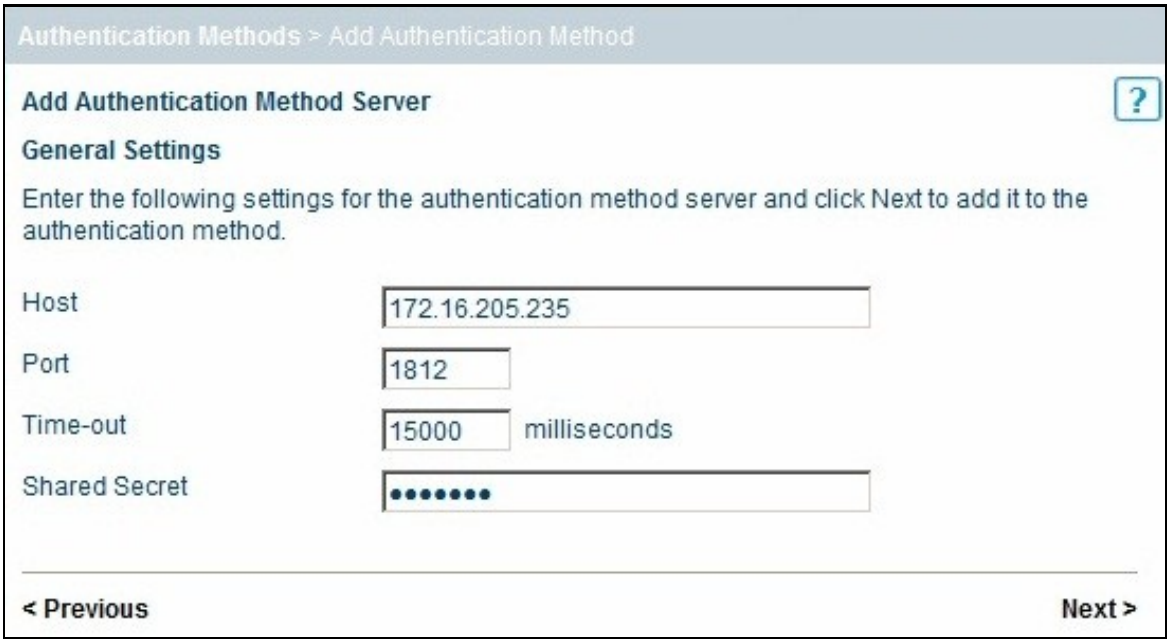
Enter the following information and when complete click Next:

Host: Hostname/IP address of the Swivel server

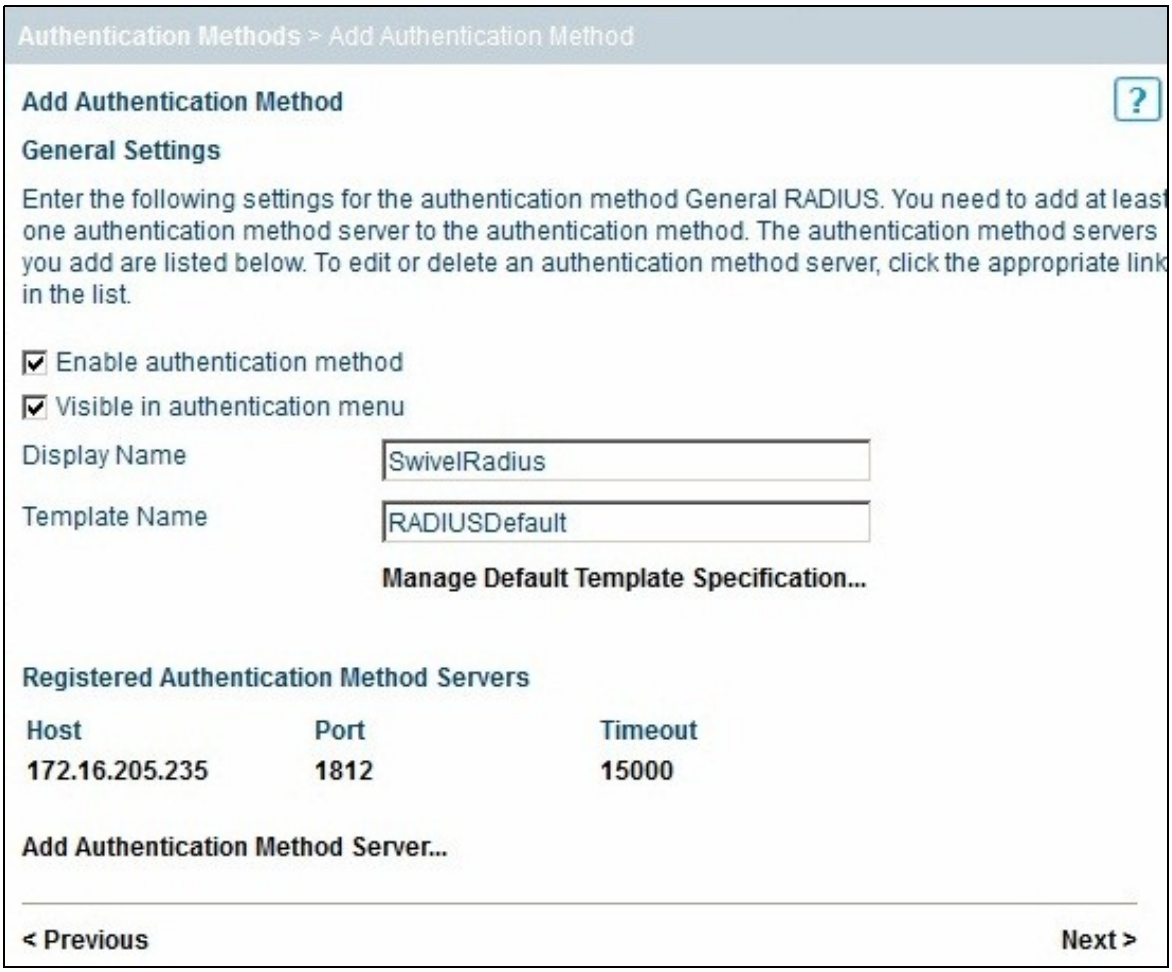
Port: RADIUS authentication port, 1812 is the default for Swivel

Time-out: default 15000 milliseconds

Shared Secret: The shared secret entered on the Swivel NAS entry for the Stonesoft server

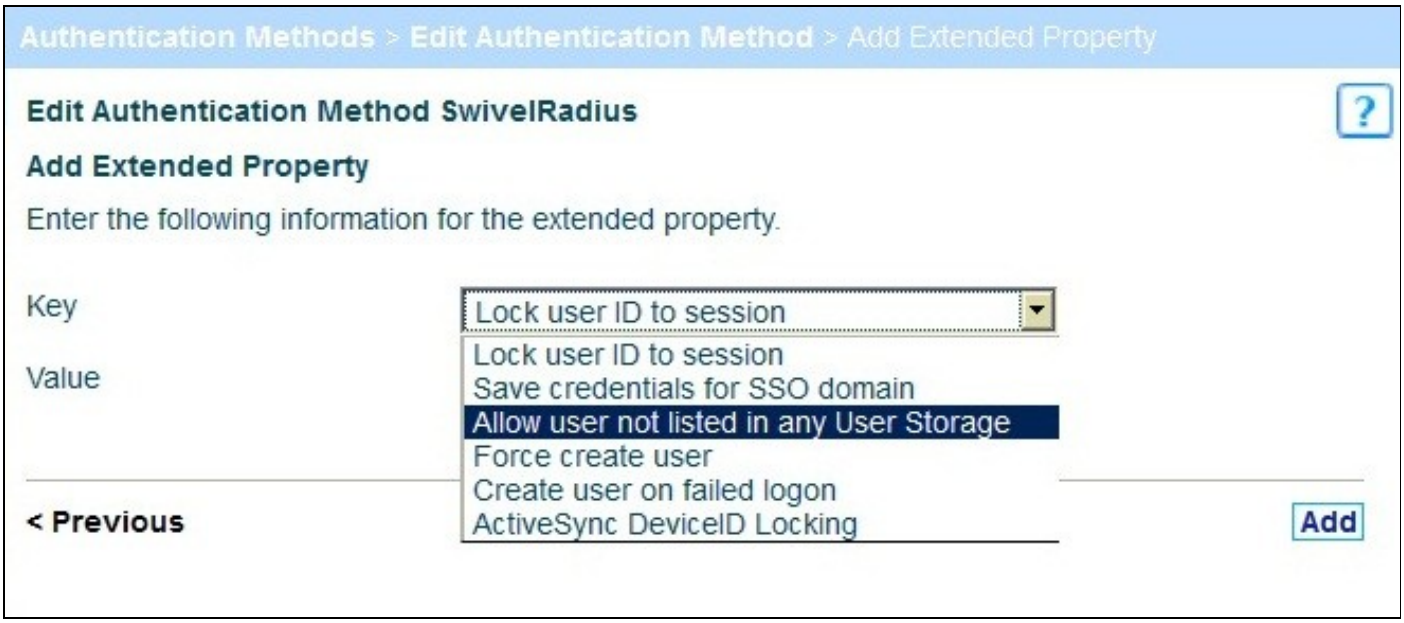


Leave the RADIUS Reply settings as default unless a specific RADIUS configuration is required



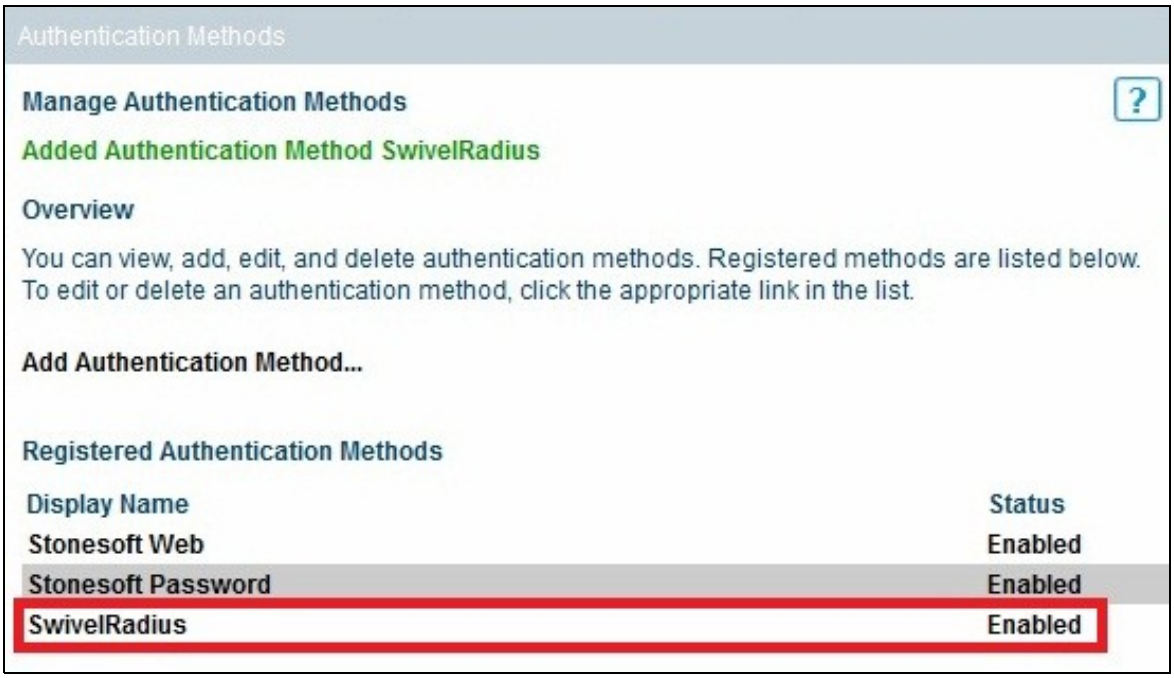
On the Extended Properties page click on Add Extended Property then select *Allow user not listed in any User Storage* and set it to *true*

The *Reveal RADIUS reject reason* can be used for troubleshooting if set to true.

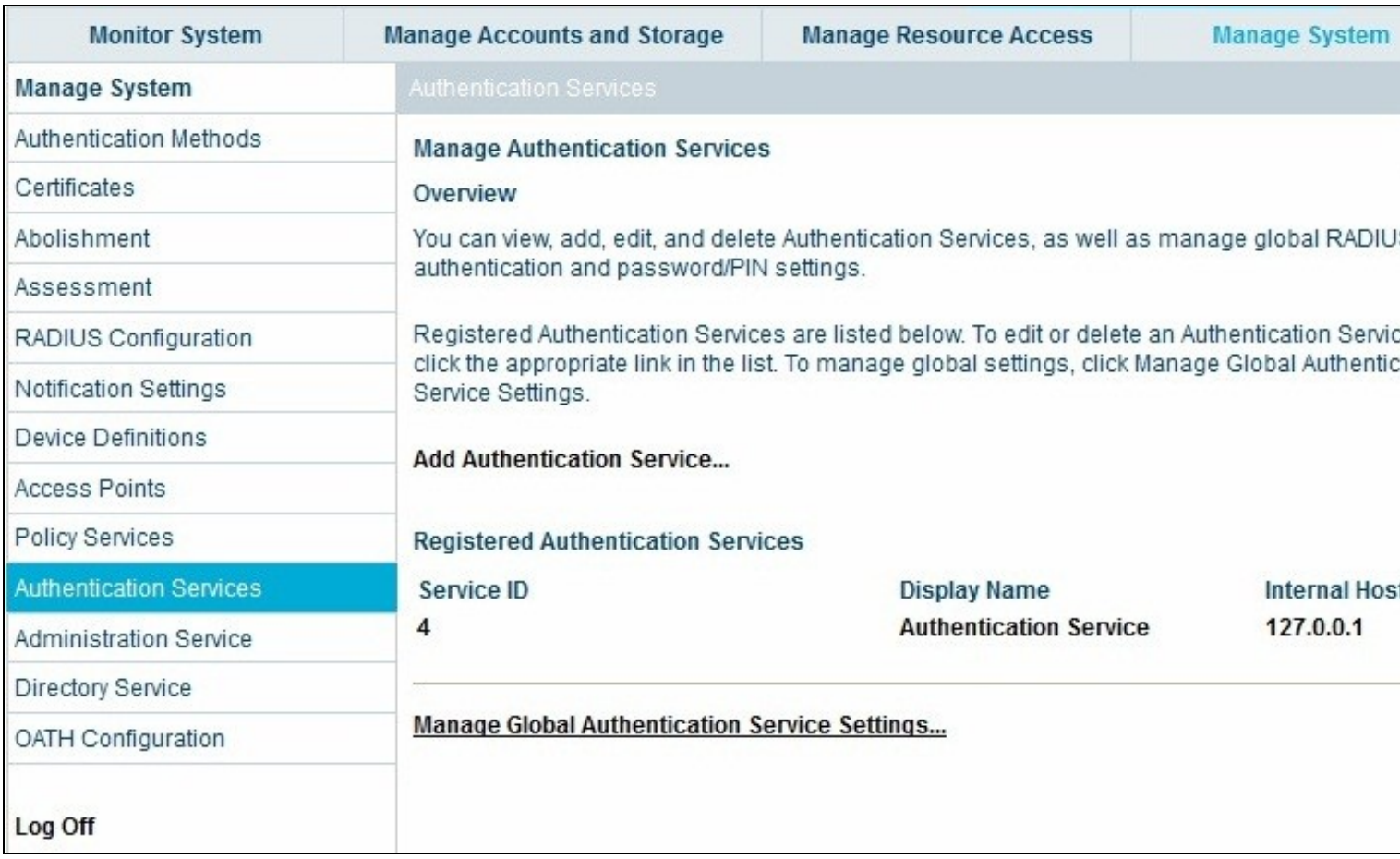


possibly not use: Stonesoft Authentication Method RADIUS Extended Properties.jpg

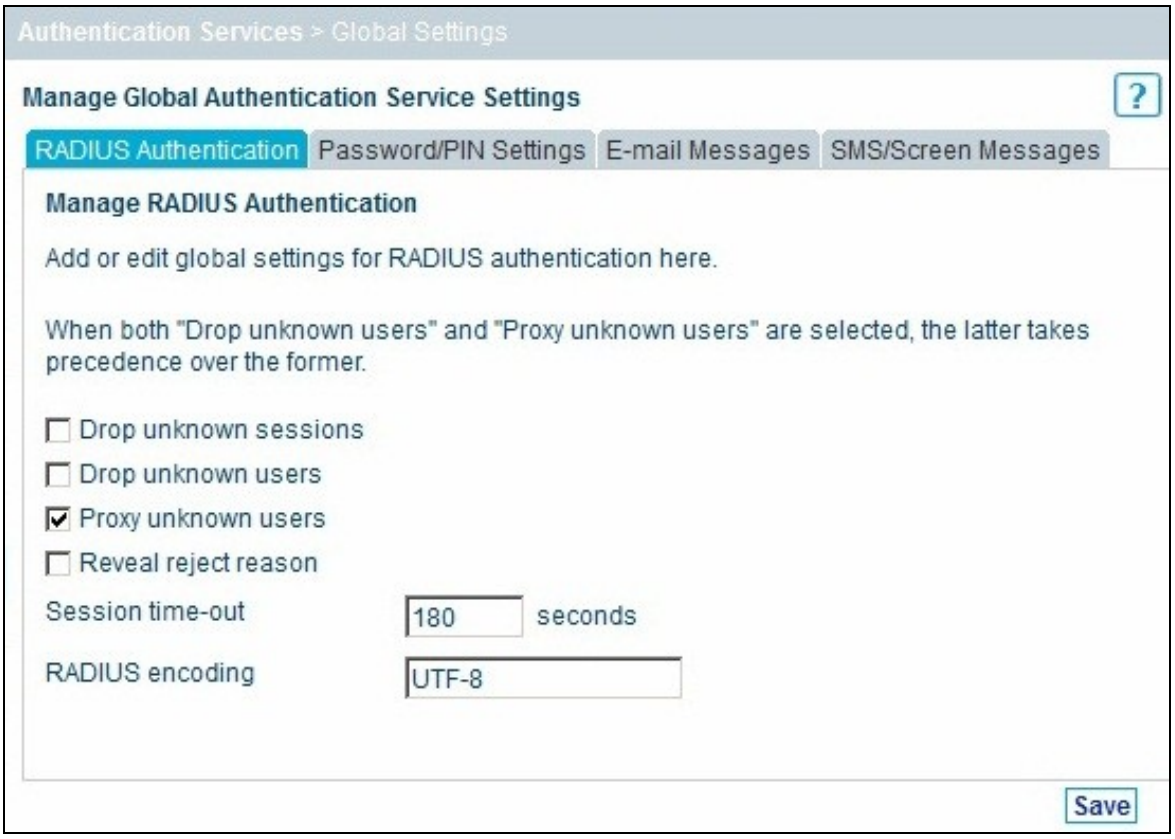
The configured RADIUS authentication method will appear under the list of *Registered Authentication Methods*.



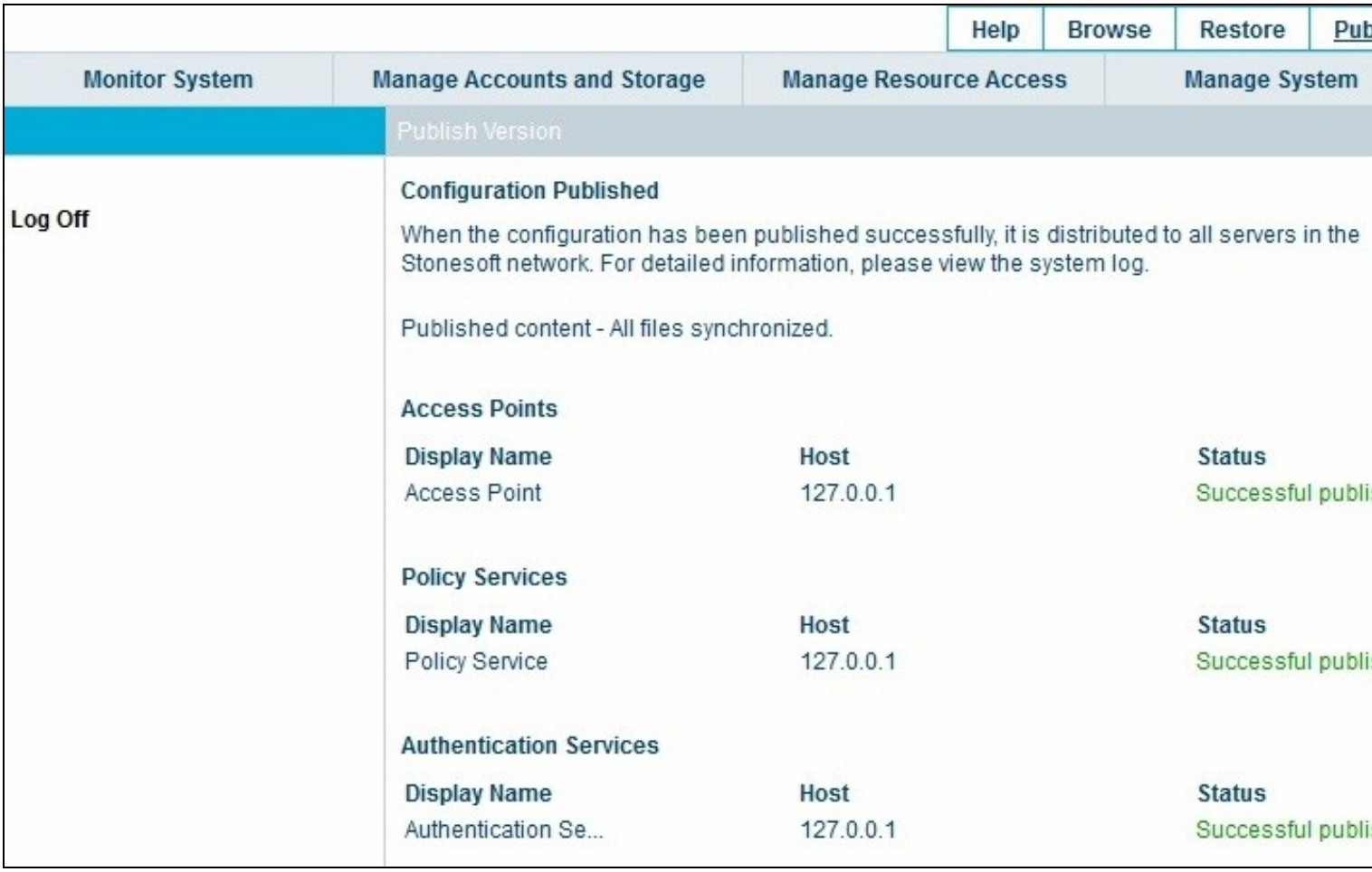
Select *Authentication Services* then *Add Authentication Service*



On the RADIUS Authentication tab, ensure that *Proxy unknown users* is checked.



When the configuration is complete then select publish



Optional: Create a Secondary Authentication Server

These modifications are used only if some of the single channel features are required. The prerequisites section contains login pages for TURing and PINpad.

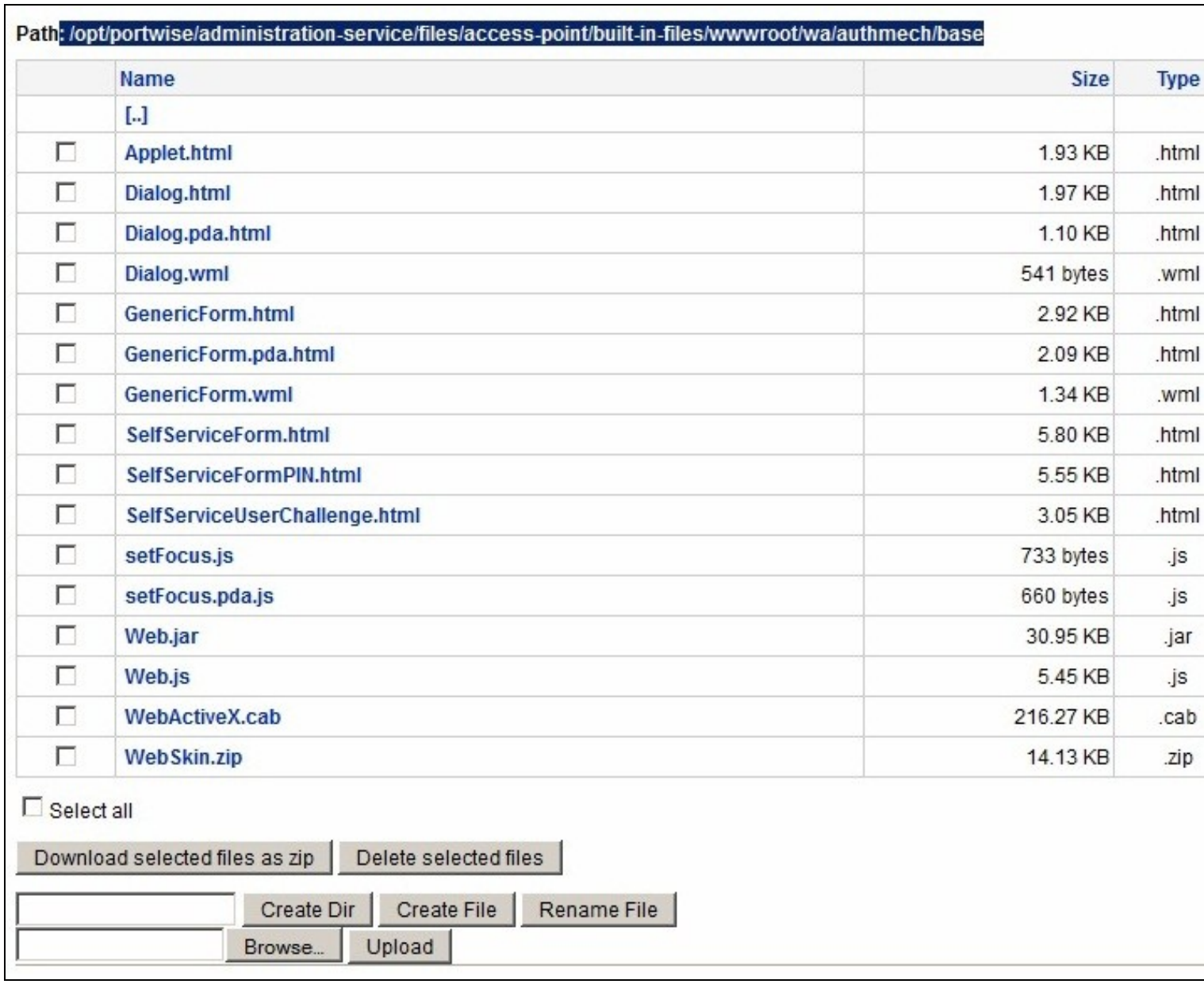
Login Page Customisation

The login page, **GenericForm.html** can be modified to allow a variety of different login methods.

To select a different login page browse to the files in:

```
/opt/portwise/administration-service/files/access-point/built-in-files/wwwroot/wa/authmech/base
```

select *browse* to select the source file, then click on *Upload*

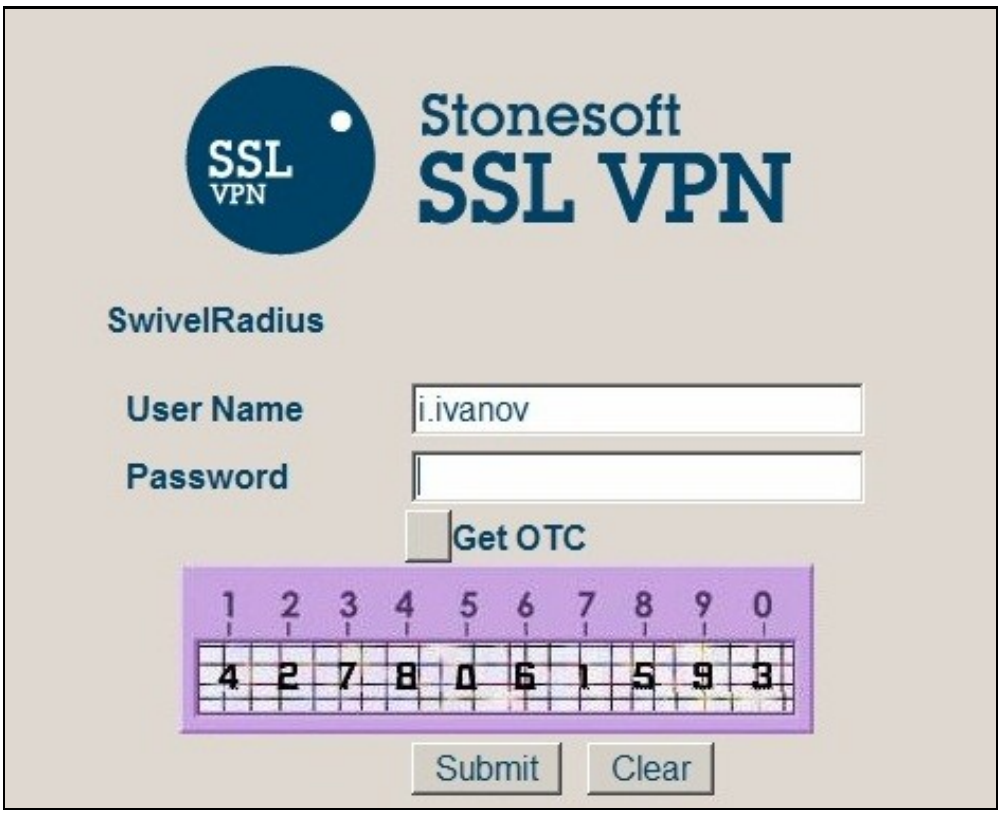


Testing

Browse to the login page and view the login page for the required configuration.

Stonesoft login page with Dual Channel using SMS, Mobile Client

Stonesoft login page with Single Channel TURing image



Stonesoft login page with PINpad

Additional Configuration Options

Two Stage Authentication

Swivel can be configured under the RADIUS/NAS settings to use Two Stage Authentication, whereby a password is entered and if correct the user is then prompted for a One Time Code, either from a graphical TURing image, mobile phone client or a Challenge and Response SMS sent to the user.

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

Known Issues and Limitations

None

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