SonicWall SSL VPN PINsafe integration

Table of Contents

1. Introduction

The SonicWALL SSL VPN can provide Dual Channel Two Factor and strong Single Channel Authentication using RADIUS.
If Strong authentication is required using Single Channel such as TURing, then the image can be displayed in the login page. The image is served from the PINsafe server to the client.

2. Overview

2.1. Prerequisites

PINsafe 3.x configured with users and SMS gateway
SonicWALL SSL VPN
PINsafe login script for the SonicWall SSL VPN

2.2. Baseline

PINsafe 3.6
SonicWall SSL VPN

2.3. Architecture

The SSL VPN appliance and the PINsafe server are usually located within the DMZ.

3. Installation

3.1. Configuring the PINsafe server

Configure a RADIUS NAS entry (if using RADIUS)

1. Ensure the RADIUS server is running on PINsafe
2. On the PINsafe Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the SonicWall SSL VPN internal IP address
5. Enter the shared secret
6. Click on Apply to save changes

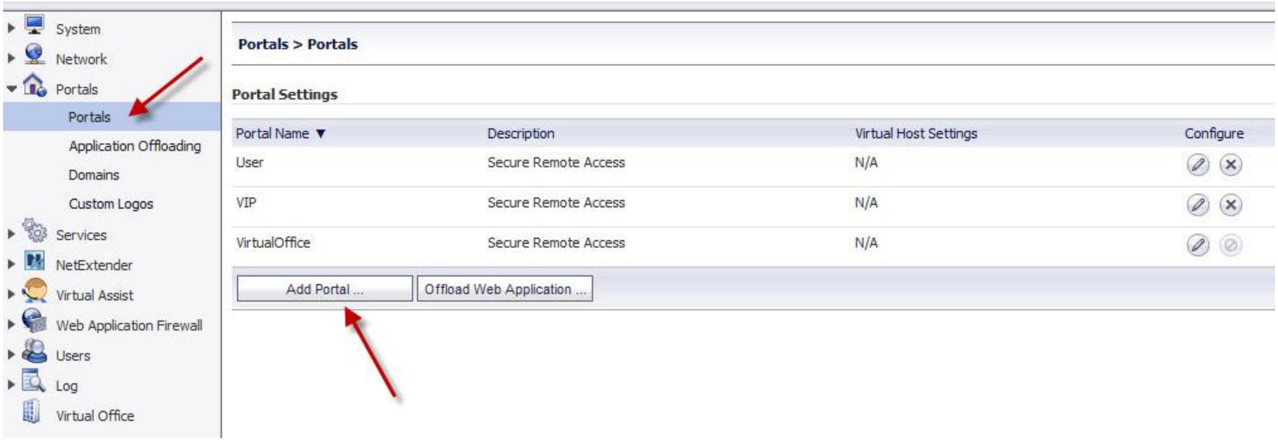
Configure Single Channel Access if required.

1. On the PINsafe Management Console select Server/Single Channel
2. Ensure ‘Allow session request by username’ is set to YES

3.2. Configuring the SonicWALL SSL VPN Appliance

3.2.1. Configuring the SonicWALL SSL VPN Portal

On the SonicWall SSL VPN select Portals, then click on Add Portal to open the add portal page.



Portal Name ▼	Description	Virtual Host Settings	Configure
User	Secure Remote Access	N/A	
VIP	Secure Remote Access	N/A	
VirtualOffice	Secure Remote Access	N/A	

Enter the following information:

Portal Name: Name for the Portal, Example, PINsafe
Portal Site Title: Name for Portal Site, Example Virtual Office
Portal Banner Title: Name for Page, Example Virtual Office
Login Message: optional login message. If the Single channel TURing image is to be used then the login script needs to be pasted into this section. Ensure the relevant scripts are modified with the External IP NAT address of the PINsafe server:

```
$('#psImage').attr('src',
'https://192.168.0.35:8443/proxy/SCImage?username=' +
encodeURIComponent(username));
```

For a PINsafe appliance this would need to be:

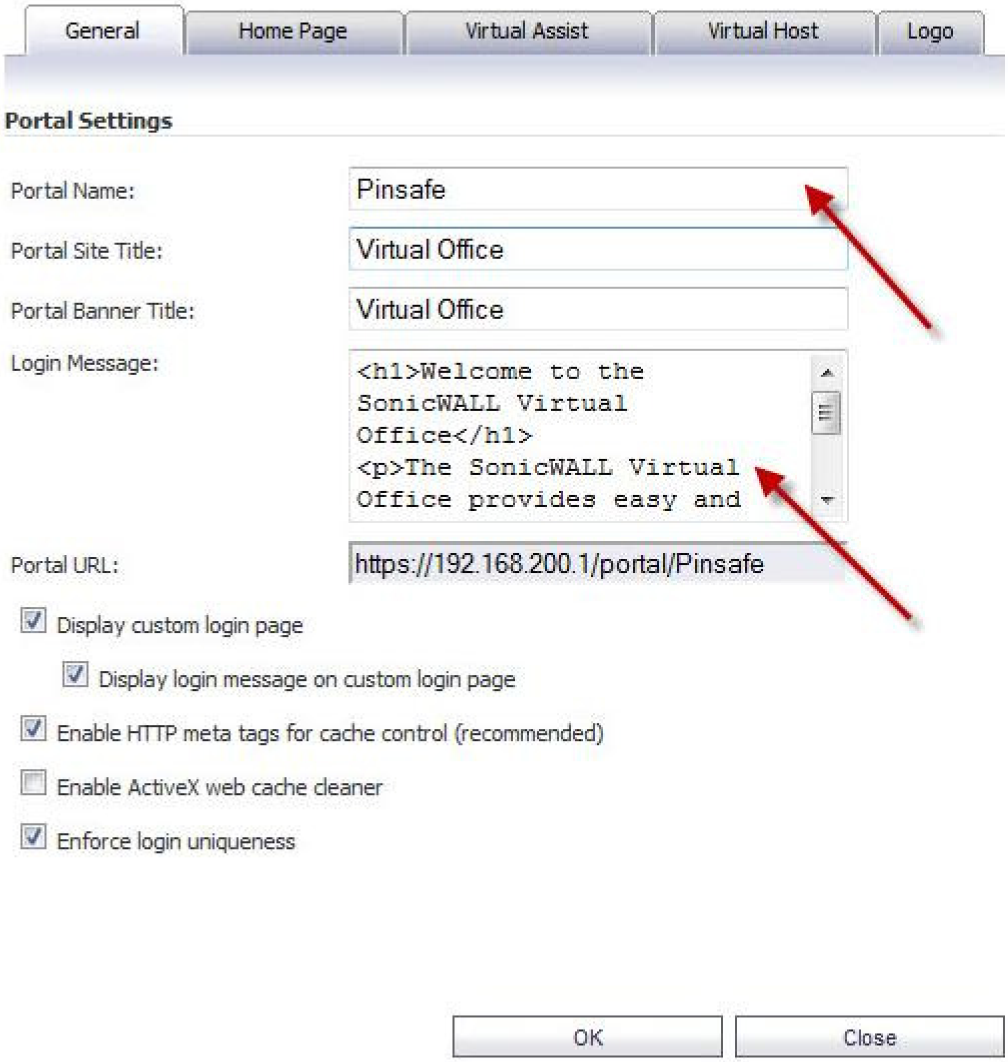
```
https://192.168.0.35:8443/proxy/SCImage?username=
For a PINsafe software only install this would be similar to:

https://192.168.0.35:8080/pinsafe/SCImage?username=
```

Portal URL: The name of the login portal

Display custom login page: Ensure this is ticked
Display login message on custom login page: Ensure this is ticked
Enable HTTP meta tags for cache control (recommended): Usually selected
Enable ActiveX web cache cleaner: Optional
Enforce login uniqueness: Ensure this is ticked

Click OK to save the settings.



Portal Settings

Portal Name: Pinsafe

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the
SonicWALL Virtual
Office</h1>
<p>The SonicWALL Virtual
Office provides easy and
```

Portal URL: https://192.168.200.1/portal/Pinsafe

☑ Display custom login page

☑ Display login message on custom login page

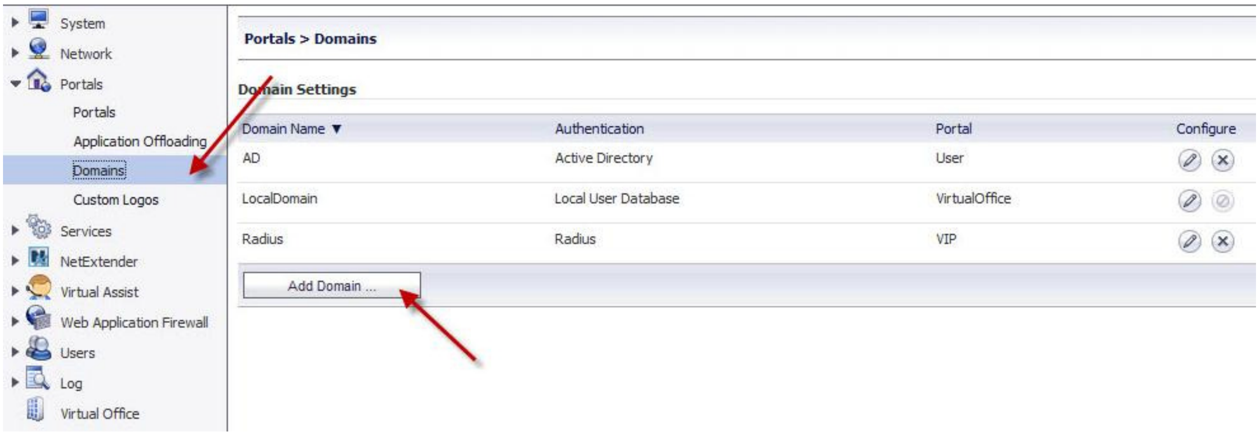
☑ Enable HTTP meta tags for cache control (recommended)

☐ Enable ActiveX web cache cleaner

☑ Enforce login uniqueness

3.2.2. Configuring the SonicWALL SSL VPN Domain Settings

On the SonicWall SSL VPN select Portals then domains and click on Add Domain.



Portals > Domains

Domain Settings

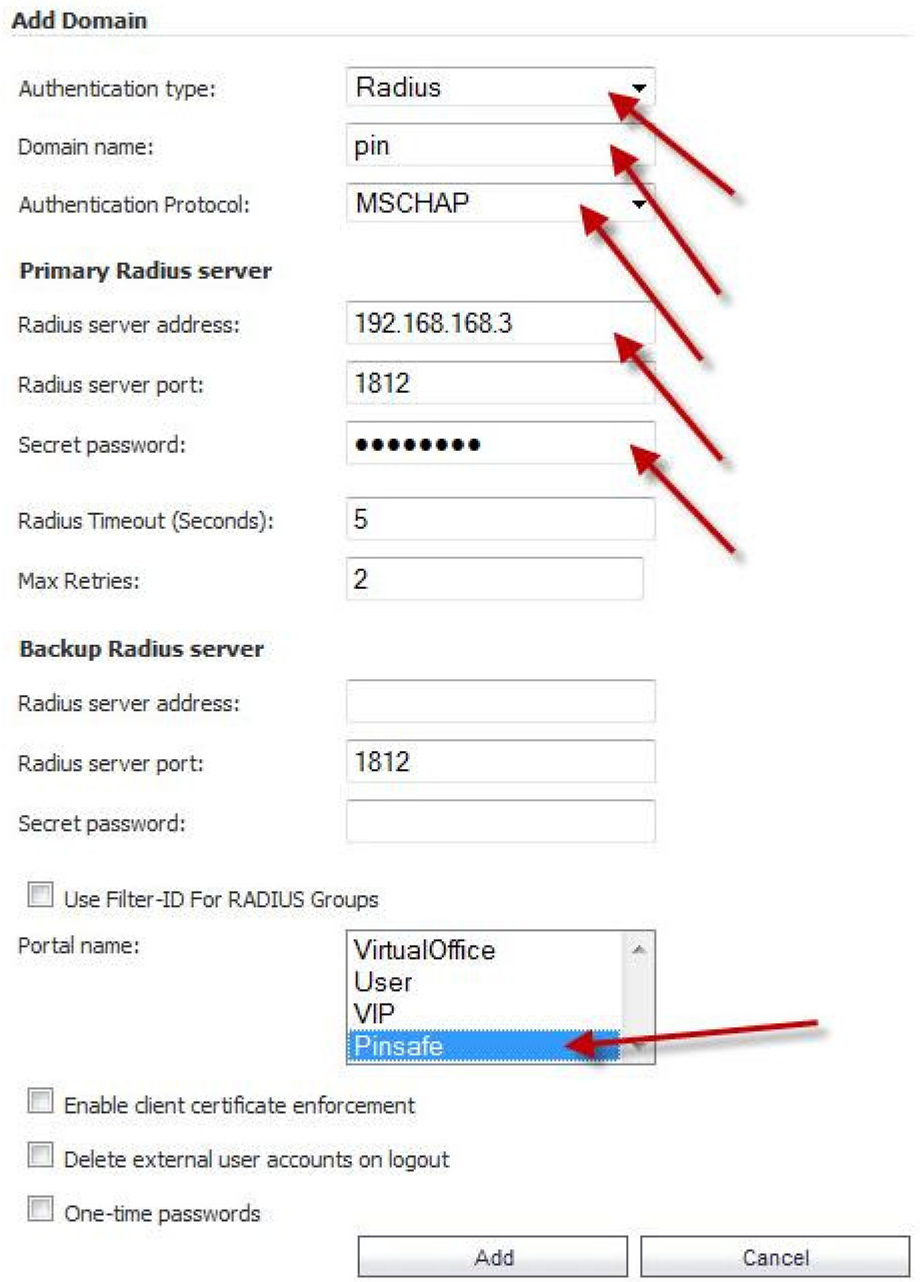
Domain Name ▼	Authentication	Portal	Configure
AD	Active Directory	User	
LocalDomain	Local User Database	VirtualOffice	
Radius	Radius	VIP	

On the Add Domain page configure the Authentication server

Authentication type: select RADIUS
Domain name: Name for the domain

Authentication Type: Select the required authentication
RADIUS server address: Hostname or IP address of the PINsafe server
RADIUS server port: Usually 1812
Secret password: Enter a shared secret that needs to be also entered on the PINsafe server NAS entry
Portal Name: Select the Portal Name created above.

Click OK to save the settings.



Add Domain

Authentication type: Radius
Domain name: pin
Authentication Protocol: MSCHAP

Primary Radius server

Radius server address: 192.168.168.3
Radius server port: 1812
Secret password: ●●●●●●●●
Radius Timeout (Seconds): 5
Max Retries: 2

Backup Radius server

Radius server address:
Radius server port: 1812
Secret password:

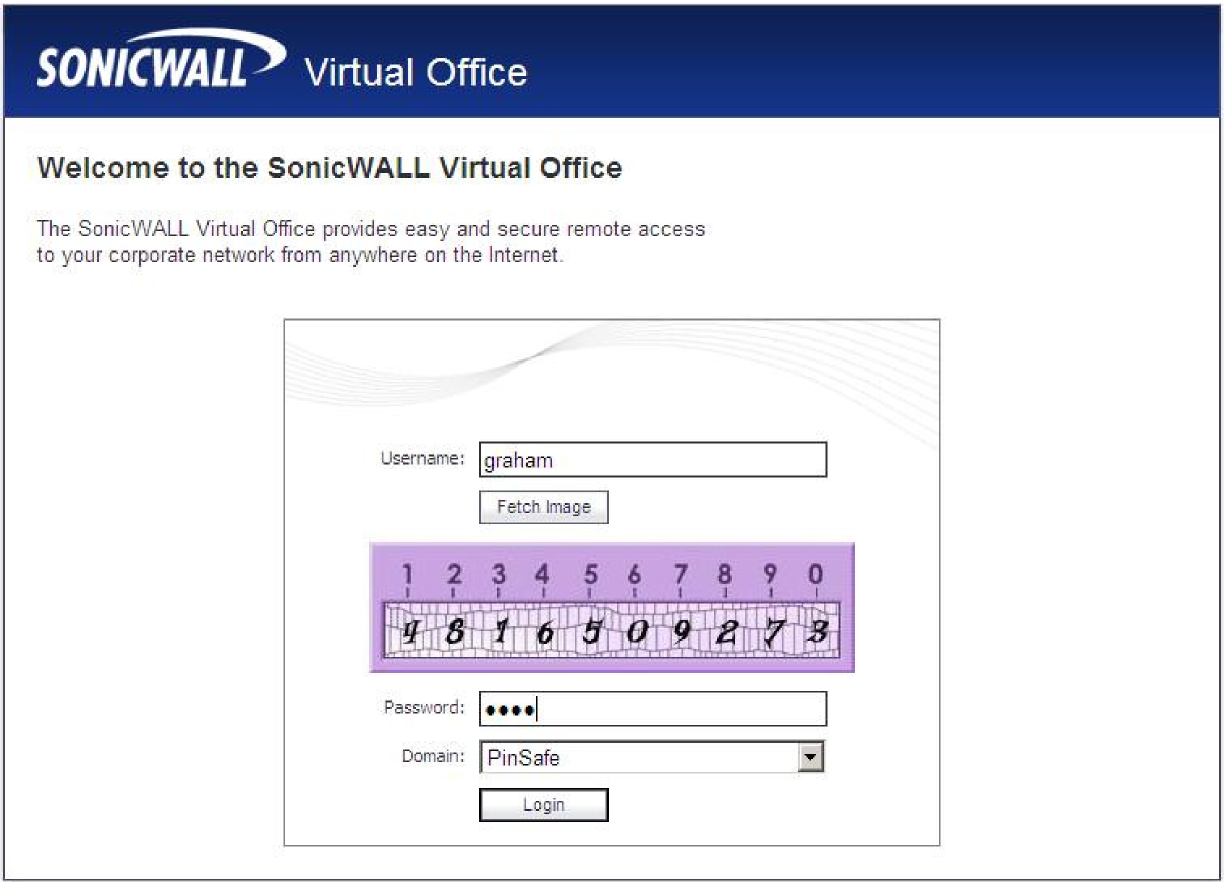
☐ Use Filter-ID For RADIUS Groups

Portal name: Pinsafe

☐ Enable client certificate enforcement
☐ Delete external user accounts on logout
☐ One-time passwords

4. Verifying the Installation

Attempt to login as a PINsafe user:



Welcome to the SonicWALL Virtual Office

The SonicWALL Virtual Office provides easy and secure remote access to your corporate network from anywhere on the Internet.

Username: graham

Password: ••••

Domain: PinSafe

5. Troubleshooting

Check the PINsafe logs

6. Known Issues and Limitations

7. 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 or the local SonicWALL office http://www.sonicwall.com/emea/Support.html.