swivelsecure

Symantec
Secure Web Gateway
Integration Guide

Swivel Secure Limited
Equinox 1, Audby Lane, Wetherby, LS22 7RD
T +44 1134 860 123 E hq@swivelsecure.com
www.swivelsecure.com

Table of Contents

Introduction

This document describes how to integrate Swivel Secure AuthControl Sentry multi factor authentication and the Symantec Secure Web Gateway (SWG) configured as a reverse proxy.

The Symantec Secure Web Gateway was previously known as the Blue Coat ProxySG, and this document is also applicable to these appliances as well.

It has been tested with the following software versions:

- **Swivel Secure AuthControl Sentry V4.x**
- **Symantec SGOS 6.7.2.1 SWG Edition**

The document focuses on the required integration steps rather than the general configuration required on both systems to meet the specific installation requirements.

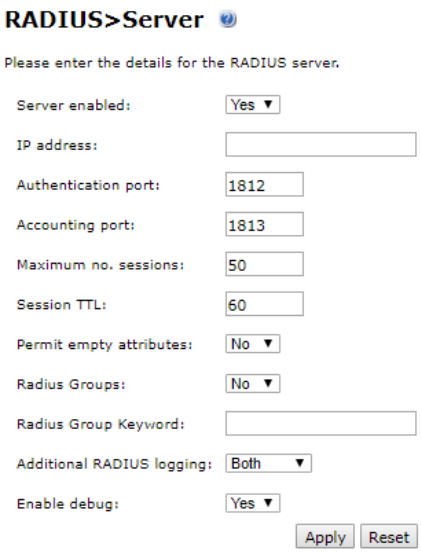
AuthControl Sentry Configuration

To configure AuthControl Sentry to integrate with the Symantec SWG you need to:

- Enable AuthControl Sentry to act as a RADIUS server
- Configure the Symantec SWG as a network access server (NAS)
- Enable the authentication image to be requested by username (not required if using the Mobile App or physical tokens)

RADIUS server configuration

From the AuthControl administration console go to RADIUS>Server and enable the service.



The IP address field is the IP address that the RADIUS server will bind to. If the IP address is left blank then the RADIUS server will service requests on all interfaces.

RADIUS NAS configuration

From the AuthControl administration console go to RADIUS>NAS.

The NAS entry consists of an Identifier, the hostname or IP address of the Symantec SWG appliance and shared secret, which will need to be matched within the SGOS configuration.

The EAP protocol should be left as None.

It is possible to restrict authentication to members of a specific AuthControl Sentry user group.

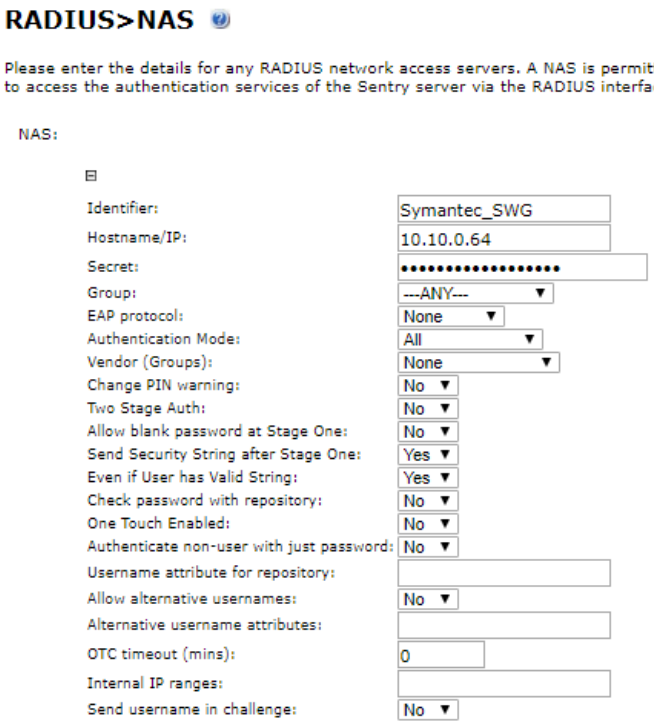
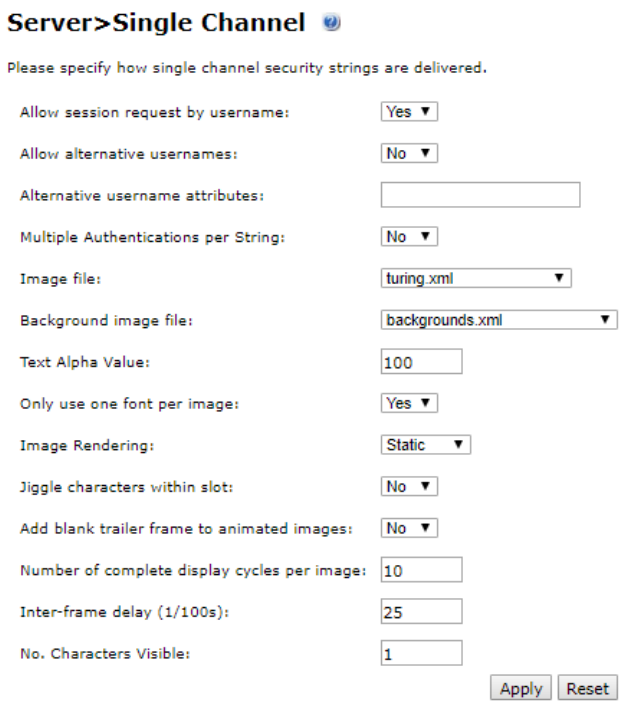


Image Request by Username

If an image based authenticator such as the TURing image is to be used then it is necessary to allow the image to be requested by specifying the username.

From the AuthControl administration console go to Server>Single Channel and set 'Allow session request by username' to Yes



Symantec SWG configuration

To configure Symantec SWG to integrate with AuthControl Sentry you need to:

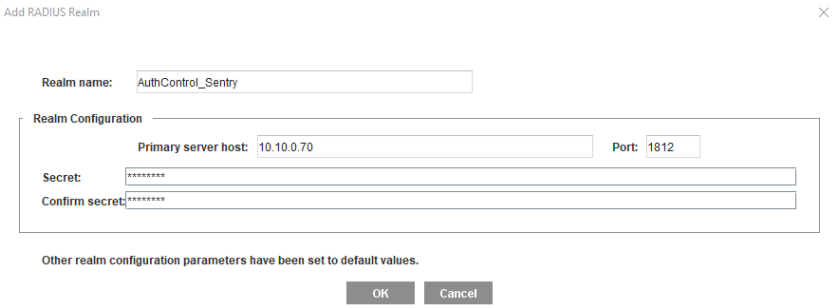
- Configure a RADIUS Authentication Realm
- Create an Authentication Form to integrate with AuthControl Sentry
- Configure a reverse proxy policy with an Authentication Layer

RADIUS Authentication Realm

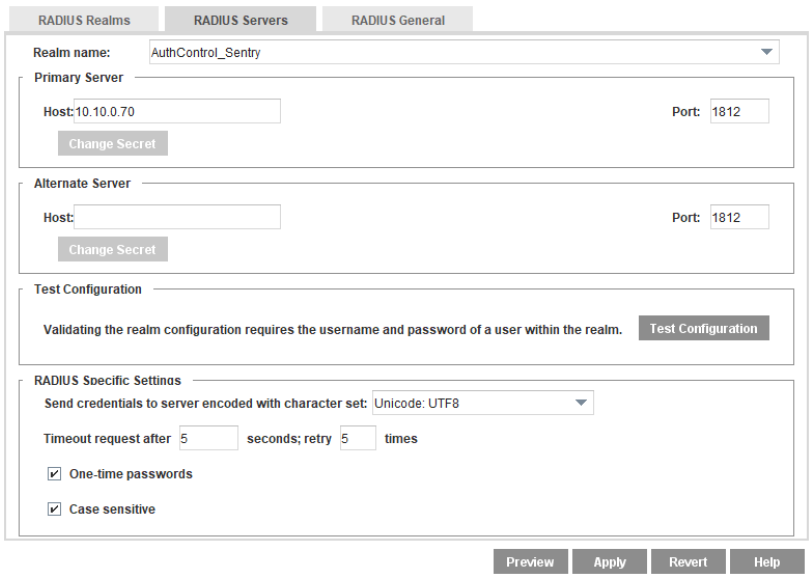
1. To create an Authentication Realm, from the Symantec SWG management console go to

   Configuration>Authentication>RADIUS>RADIUS Realms>New

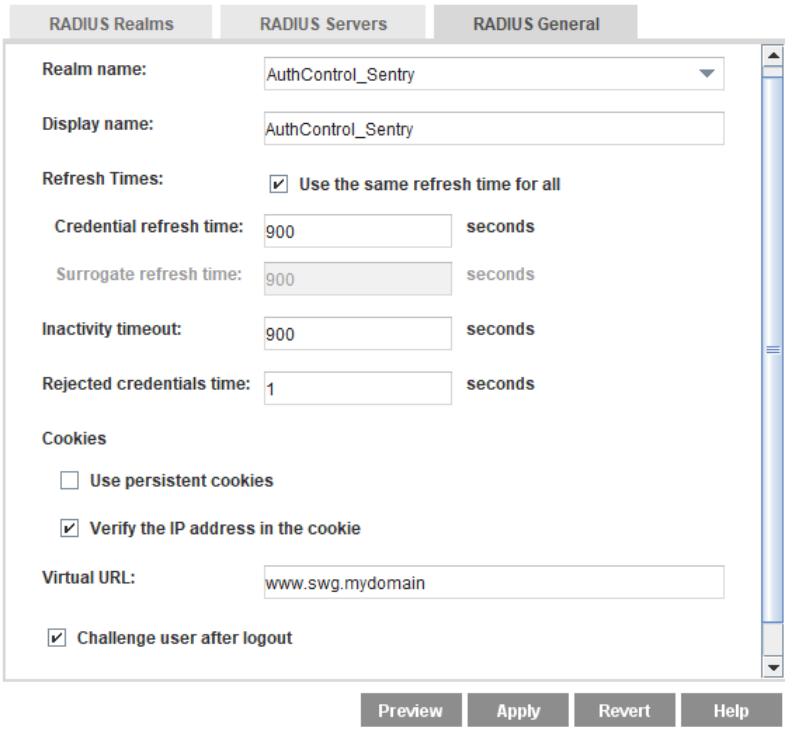
   The RADIUS Realm entry consists of an Identifier, the hostname or IP address of the AuthControl Sentry appliance and shared secret, which will need to be matched within the AuthControl Sentry configuration.



2. Select the RADIUS Servers tab and enable 'One-time passwords'. If your AuthControl Sentry is configured as a high availability pair, then enter the IP address of the second appliance in the Alternate Server>Host together with the 'Secret'.



3. Select the RADIUS>General tab and enter a 'Virtual URL'. This can be any fictitious URL, but for authentication to work the local client must be able to resolve it in DNS to an address that points to the Symantec SWG.



Then click on Apply to save the changes

Configure an Authentication Form

An Authentication Form is required to capture the user credentials. If an AuthControl Sentry Dual Channel authentication method is required, for example Mobile App (OTC), SMS or physical token, then the default 'authentication_form' will provide the basic functionality to capture the username and OTC when the user authenticates.

If it is required to use the TURing image based authenticator then the default 'authentication_form' will need to be modified as follows:

The variable sUrl must be modified with the FQDN of the AuthControl Sentry appliance.

```
<HTML>
<HEAD>
<TITLE>Enter Proxy Credentials for Realm $(cs-realm)</TITLE>
</HEAD>
<BODY>
<H1>Enter Proxy Credentials for Realm $(cs-realm)</H1>
<P>Reason for challenge: $(exception.last_error)
<P>$(x-auth-challenge-string)
<FORM METHOD="POST" ACTION=$(x-cs-auth-form-action-url)>
$(x-cs-auth-form-domain-field)
<P>Username: <INPUT NAME="PROXY_SG_USERNAME" MAXLENGTH="64" VALUE="$(cs-user)" onblur=ShowTuring()></P>

<P>Password: <INPUT TYPE=PASSWORD NAME="PROXY_SG_PASSWORD" MAXLENGTH="64"></P>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_REQUEST_ID" VALUE="$(x-cs-auth-request-id)">
<INPUT TYPE=HIDDEN NAME="PROXY_SG_PRIVATE_CHALLENGE_STATE" VALUE="$(x-auth-private-challenge-state)">

<P><INPUT TYPE=SUBMIT VALUE="Submit"> <INPUT TYPE=RESET onclick=HideTuring()></P>
</FORM>

<P><img id=imgTuring name=imgTuring border="1" style='visibility:hidden'></P>
<P><input type=button id=btnRefreshTuring name=btnRefeshTuring value="Refresh Image" style='visibility:hidden'
onclick=ShowTuring()></P>
<P>$(exception.contact)</P>

<script language="javascript">

var sName = "PROXY_SG_USERNAME";
var sPassword = "PROXY_SG_PASSWORD"
var sUrl = "https://a.b.c.d:8443/proxy/SCImage?username=";
varImg = document.getElementById("imgTuring");
varRefresh = document.getElementById("btnRefreshTuring");

function ShowTuring() {
 sUser=document.getElementsByName(sName)[0].value;
 if (sUser=="") {
 alert ("Please enter your username first!");
 document.getElementsByName(sName)[0].focus()
 }
 else
 {

 //Set the TURing image SRC and make it visible
 varImg.src = sUrl + sUser + "&random=" + Math.floor(Math.random()*100000);
 varImg.style.visibility = "visible";
 varRefresh.style.visibility = "visible";

 //Set focus to the OTC input
 document.getElementsByName(sPassword)[0].focus()
 }
}
function HideTuring(){
 varImg.style.visibility = "hidden";
 varRefresh.style.visibility = "hidden";
}
 </script>
</BODY>
</HTML>
```

Once the required modified form has been created in a local text file, it needs to be uploaded to the SWG appliance.

1. From the Symantec SWG management console go to

   Configuration -> Authentication ->Forms

2. Select 'New', select 'Authentication Form' and give it a name.
3. Select the new form you that you have created, select 'Edit'
4. Select 'Local File' and 'Install'.

5. Browse to the file you have created and upload it.
6. Click 'Apply' to save the changes made.

Create a reverse proxy with authentication policy

This aspect of the configuration is dependent on how you are deploying the Symantec SWG Proxy and what elements you wish to secure with AuthControl Sentry authentication. This example illustrates using AuthControl Sentry authentication to protect access to a specific web application where the Symantec SWG is acting as a reverse proxy.

It is assumed that the SWG appliance has already been configured as a reverse proxy for the web application that needs to be protected with AuthControl Sentry.

The following steps are required before the reverse proxy policy can be created:

- Create a Virtual IP on the network interface that clients will connect to
- Create Forwarding Hosts entries to define the web application servers

Refer to the Symantec SWG documentation for detailed information on how to configure the reverse proxy.

The policy configuration is created from within the Visual Policy Manager (VPM), and the following policy layers are required:

- Web Access Layer
- Forwarding Layer
- Web Authentication Layer

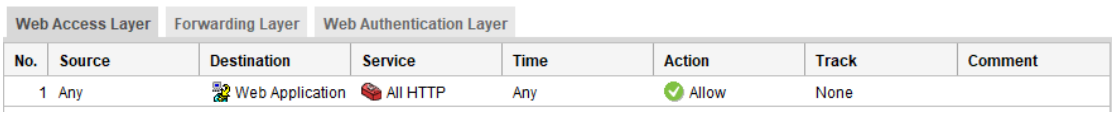
Web Access Layer

Create a rule:

- Source: ANY
- Destination: Web Application

  (create an URL Object that matches the external URL or IP address that clients will connect to – this should match the VIP address that was configured earlier)

- Service: As required by the application (usually HTTP or HTTPS)
- Time: ANY
- Action: Allow



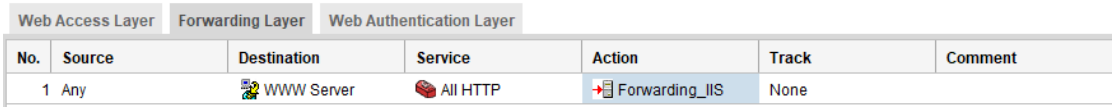
Forwarding Layer

Create a rule:

- Source: ANY
- Destination: Web Server

(create an URL Server Object that matches the external URL or IP address that clients will connect to – this should match the VIP address that was configured earlier)

- Service: As required by the application (usually HTTP or HTTPS)
- Action: Forward
- (create a Forwarding object that proxies all traffic destined for the VIP address to the web application – this is defined in the Forwarding Host(s) section.



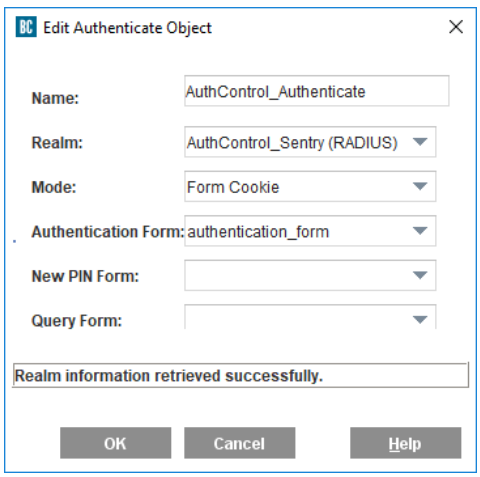
Web Authentication Layer

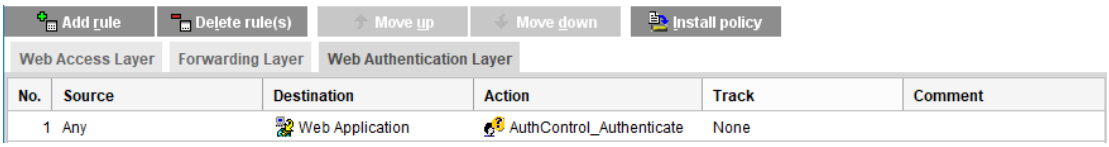
Create a rule:

- Source: ANY
- Destination: Web Application (previously defined URL Object)
- Action: AuthControl_Authenticate (see object definition below)

Create an Authenticate Object:

- Name: AuthControl_Authenticate
- Realm: AuthControl_Sentry (RADIUS)
- Mode: Form Cookie (preferred mode for reverse proxy use)
- Authentication Form: authentication_form (use this for basic OTC or select the custom form created previously for the TURing image)



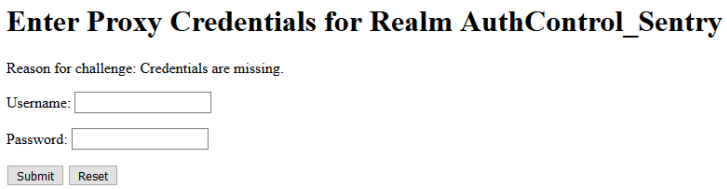


Install the policy

Testing the authentication

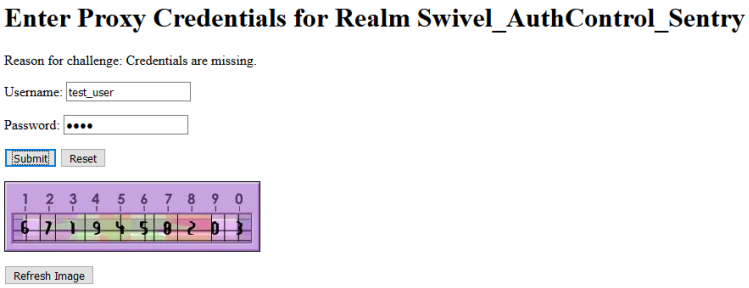
From a browser connect to the URL that resolves to the VIP address that is configured on the Symantec SWG.

If using the default authentication form, you will be presented with this page:



Enter the Username (as the user is defined in AuthControl Sentry), and for the Password enter the OTC. If successful then you will be proxied through to the web application.

If using the modified authentication form to display the TURing image you will be presented with this page:



Enter the Username (as the user is defined in AuthControl Sentry), and then the TURing image will be automatically displayed below. Then with the user's PIN, extract the OTC and enter it into the Password field. If successful then you will be proxied through to the web application. The 'Refresh Image' button will allow a new image to be displayed, should the user be unable to distinguish the numerals in the image.