Sentry SSO with Cisco ASA

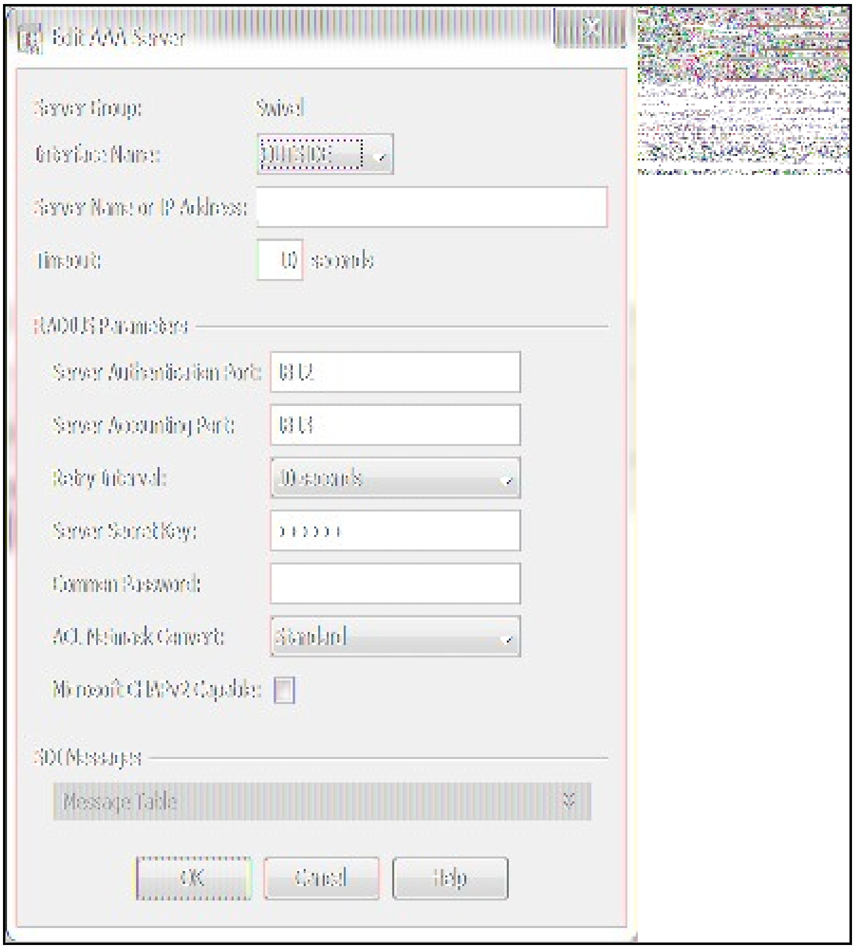
Contents

Introduction

This Document describes how to integrate a Cisco ASA with Swivel Sentry SSO. As Cisco ASA does not support SAML natively, this uses a custom login page to redirect to Sentry, and RADIUS to verify that the SAML claim is valid. Therefore, this solution is not suitable for use with AnyConnect.

Configure Cisco ASA

The first step is to create a RADIUS authentication server group, and associate it with a connection profile. We do not go into details on this, as we presume the customer is familiar with configuring a Cisco ASA. However, please ensure that the server is set to match the Swivel IP address or host name. Note that the Swivel appliance doesn't support using a virtual IP address with RADIUS. Also, check that the ports match those on the Swivel RADIUS server (the defaults are 1812 and 1813, which should be correct). Make a note of the Server Secret Key used, as this will need to be entered on the Swivel server. Do not enable the **Microsoft CHAPv2 Capable** option.



Edit AAA Server

Server Group: Swivel

Interface Name: OUTSIDE

Server Name or IP Address:

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1812

Server Accounting Port: 1813

Retry Interval: 10 seconds

Server Secret Key: ******

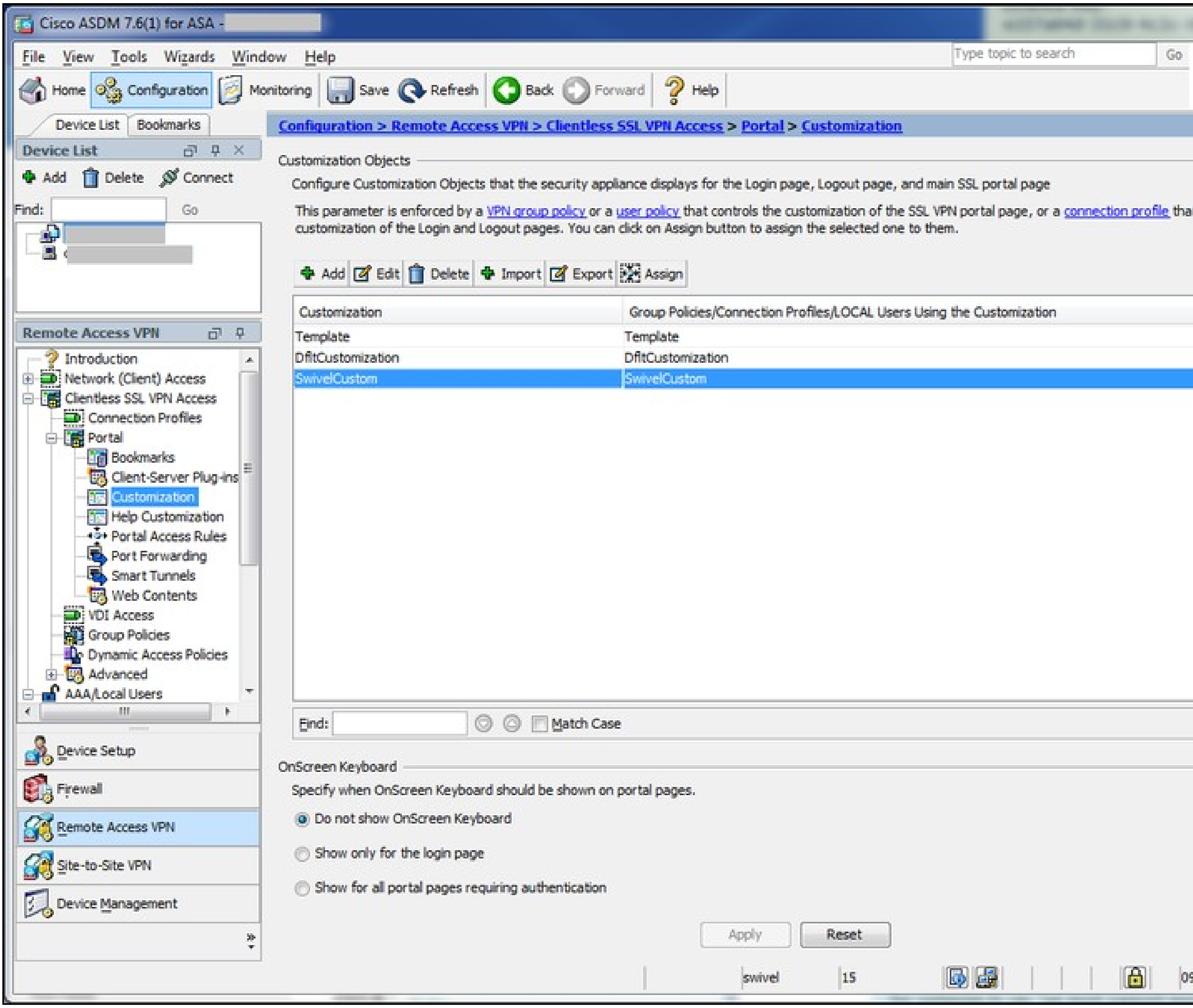
Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: □

SDI Messages

You will now need to customize the web page, as follows:



Configure Customization Objects that the security appliance displays for the Login page, Logout page, and main SSL portal page

This parameter is enforced by a VPN group policy or a user policy that controls the customization of the SSL VPN portal page, or a connection profile tha customization of the Login and Logout pages. You can click on Assign button to assign the selected one to them.

Customization	Group Policies/Connection Profiles/LOCAL Users Using the Customization
Template	Template
DfltCustomization	DfltCustomization
SwivelCustom	SwivelCustom

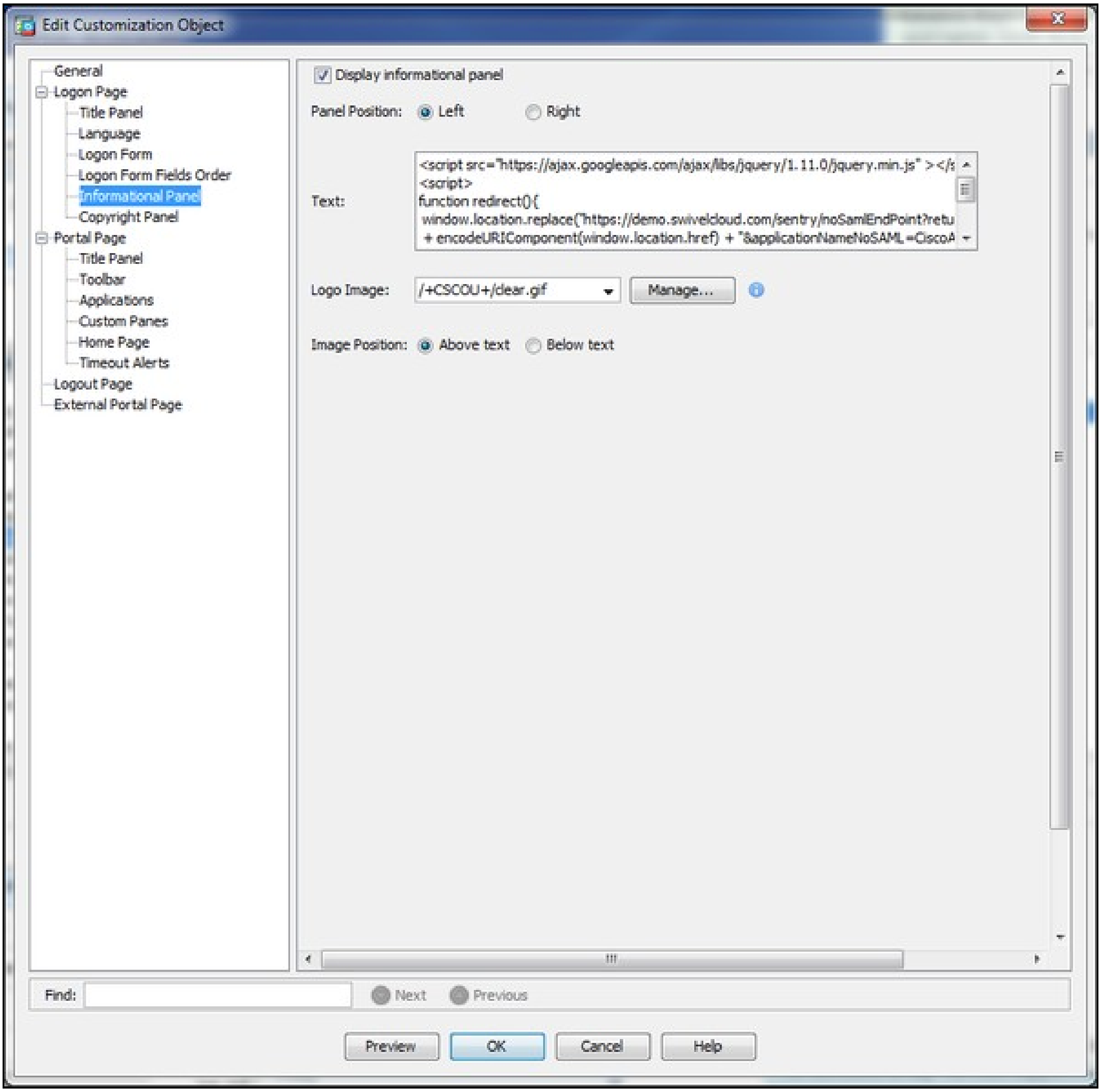
Specify when OnScreen Keyboard should be shown on portal pages.

● Do not show OnScreen Keyboard

○ Show only for the login page

○ Show for all portal pages requiring authentication

Select the customization you intend to use, or create a new one. If you create a new one, make sure you associate it with the connection profile that uses the Swivel server, on the **General** tab.



☑ Display informational panel

Panel Position: ● Left ○ Right

Text:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></s
<script>
function redirect(){
 window.location.replace("https://demo.swivelcloud.com/sentry/noSamlEndPoint?retu
 + encodeURIComponent(window.location.href) + "&applicationNameNoSAML=CiscoA
```

Logo Image: /+CSCOU+/clear.gif Manage...

Image Position: ● Above text ○ Below text

Select **Informational Panel**. Make sure you check **Display informational panel**. Then paste the following code in the **Text** field:

```
 <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
 <script>
 function redirect(){
   window.location.replace("https://<swivel_server>/sentry/noSamlEndPoint?returnurlNoSAML="
     + encodeURIComponent(window.location.href) + "&applicationNameNoSAML=<EntityID>" );
 }
 var QueryString = function () {
   // This function is anonymous, is executed immediately and
   // the return value is assigned to QueryString!
   var query_string = {};
   var query = window.location.search.substring(1);
   var vars = query.split("&");
   for (var i=0;i<vars.length;i++) {
     var pair = vars[i].split("=");
     // If first entry with this name
     if (typeof query_string[pair[0]] === "undefined") {
       query_string[pair[0]] = pair[1];
     // If second entry with this name
     } else if (typeof query_string[pair[0]] === "string") {
       var arr = [ query_string[pair[0]], pair[1] ];
       query_string[pair[0]] = arr;
     // If third or later entry with this name
     } else {
       query_string[pair[0]].push(pair[1]);
     }
   }
   return query_string;
} ();

$(document).ready(function(){
  usernamePassedIn = QueryString["username"];
  passwordPassedIn = QueryString["password"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
   redirect();
  } else {
   $('[name=password]').val(claimPassedIn);
   $('[name=username]').val(usernamePassedIn);
   // $('[name=user#2]').val(usernamePassedIn);
   // $('[name=password#2]').val(claimPassedIn);
   document.getElementById("unicorn_form").submit();
 }
 });
 </script>
```

before you paste it, replace <swivel_server> with the public host name of your Swivel Sentry server. Also, replace <EntityID> with the Entity ID of the Sentry application you create - see below.

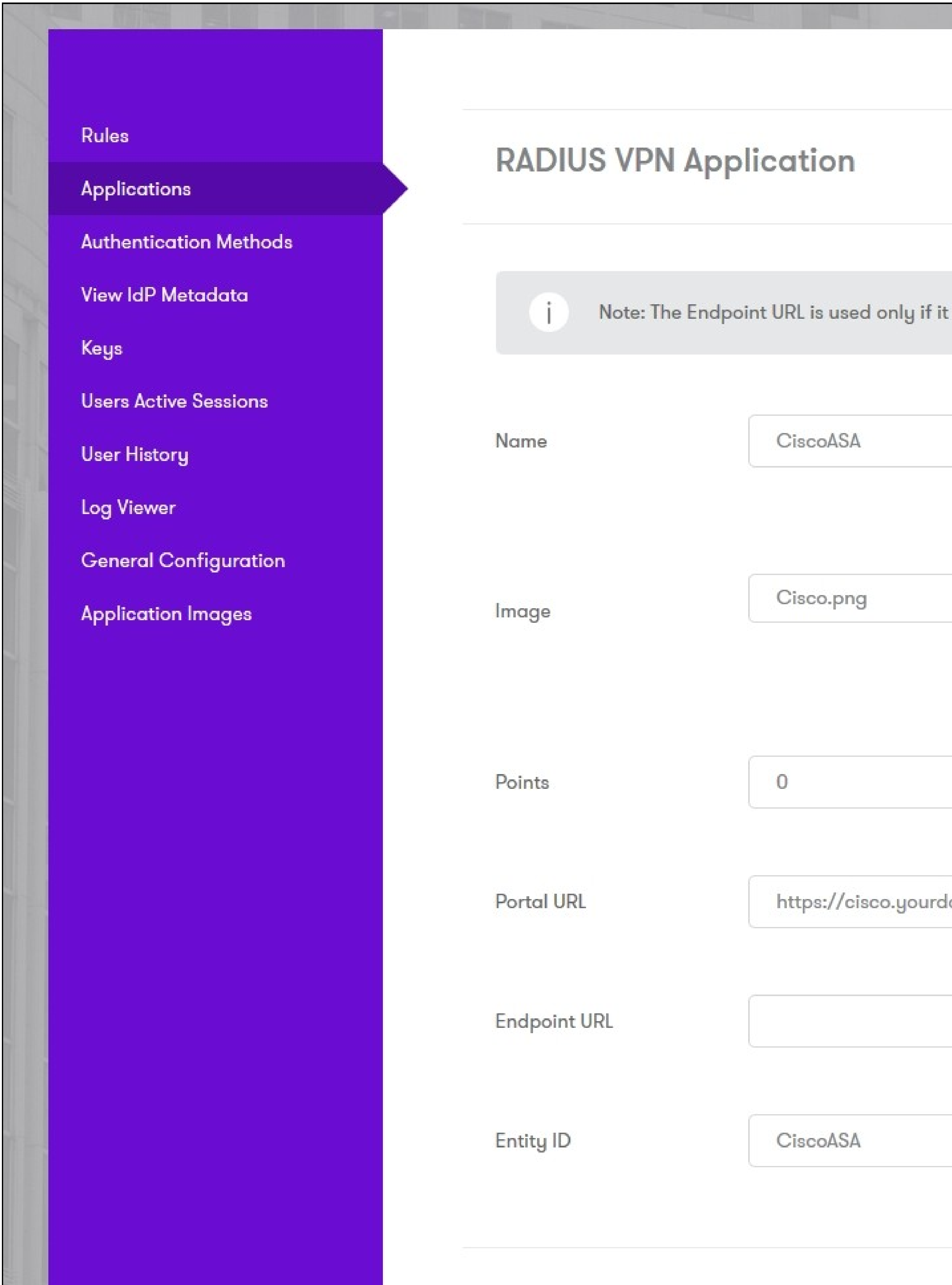
Secondly, go to the **Logout Page** tab and enter the following code:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
 window.location.replace("https://<swivel_server>/sentry/singlelogout");
}
$(document).ready(function(){
  redirect();
 });
</script>
```

Again, replace <swivel_server> with the public host name of your Swivel Sentry server.

Configure Swivel Sentry

Log into the Sentry administration console. Select **Applications**. Then click **Add Application** and select the type **RADIUS VPN - Cisco ASA**



RADIUS VPN Application

Note: The Endpoint URL is used only if it

Name	CiscoASA
Image	Cisco.png
Points	0
Portal URL	https://cisco.yourd
Endpoint URL	
Entity ID	CiscoASA

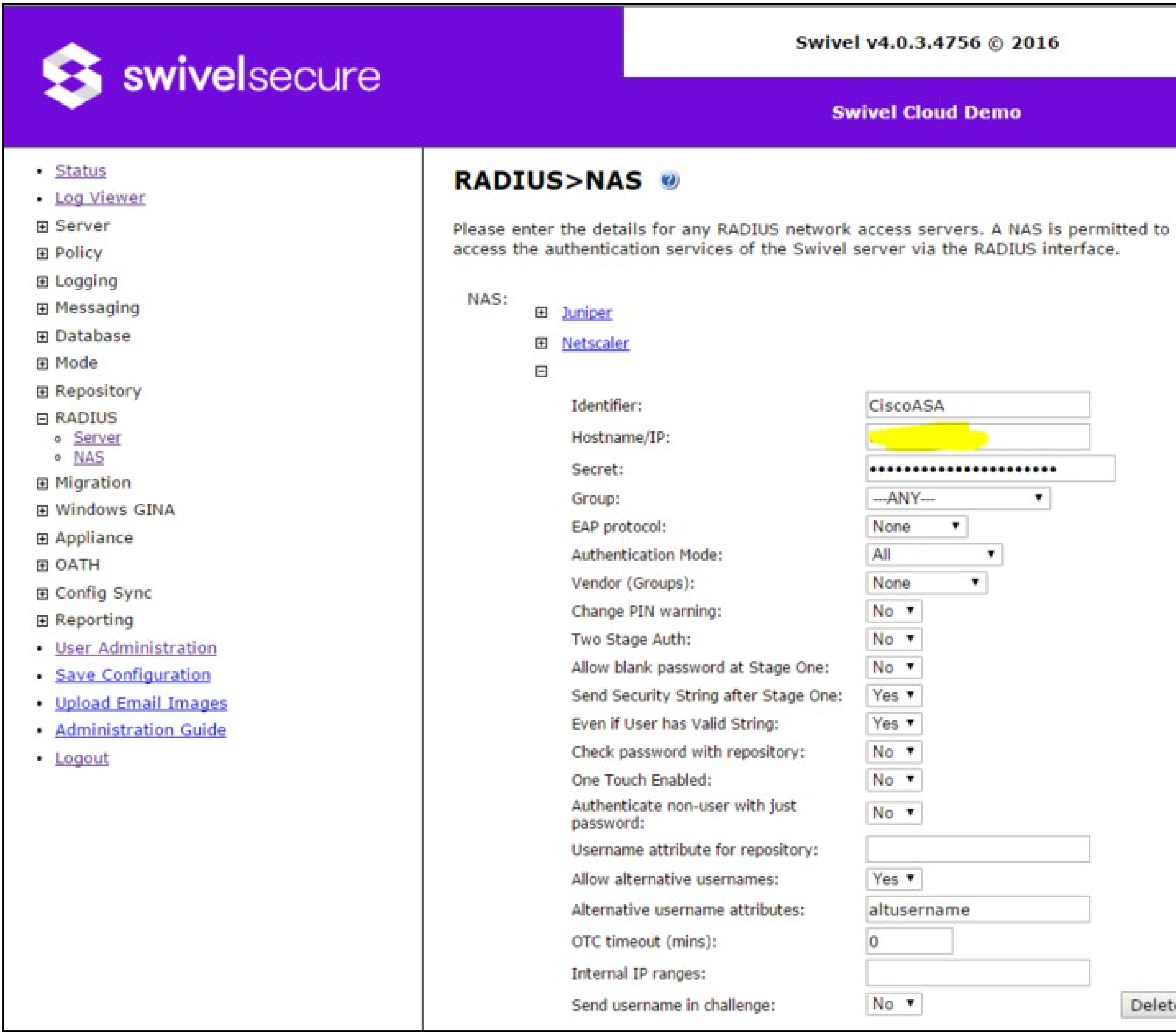
Enter a name - it is recommended that the name is the same as the Entity ID below.

Portal URL should be the public URL of your Cisco server. It is recommended that you use the same address for **Endpoint URL**, although this will usually be overridden be the address sent by the Cisco login page.

Entity ID must be the same as the value shown as *<EntityID>* in the section above, so that Sentry will recognize the request as coming from this Cisco server.

Configure RADIUS NAS on Swivel Core

You need to create a new NAS entry on the Swivel Core application. Log into the Swivel web admin console, and go to RADIUS -> NAS.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the Swivel server via the RADIUS interface.

NAS: ⊞ Juniper ⊞ Netscaler ⊟

Identifier:	CiscoASA
Hostname/IP:	[redacted]
Secret:	••••••••••••••••••••••
Group:	--ANY--
EAP protocol:	None
Authentication Mode:	All
Vendor (Groups):	None
Change PIN warning:	No
Two Stage Auth:	No
Allow blank password at Stage One:	No
Send Security String after Stage One:	Yes
Even if User has Valid String:	Yes
Check password with repository:	No
One Touch Enabled:	No
Authenticate non-user with just password:	No
Username attribute for repository:	
Allow alternative usernames:	Yes
Alternative username attributes:	altusername
OTC timeout (mins):	0
Internal IP ranges:	
Send username in challenge:	No

Identifier must be the same as the Entity ID from the Sentry application and the Cisco custom code, in order for authentication to succeed.

Hostname/IP should be the IP address (or hostname) of the Cisco ASA.

Secret must be the same as the one entered on the RADIUS server details on the Cisco.

Everything else should be left as default.

SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

Known Issues/Limitations

This method of authentication relies on the default policy for the Cisco portal requiring Swivel RADIUS authentication as the only authentication. It will not work if additional authentication is required, or if the user needs to select the Swivel authentication policy.

Because this method uses a custom login page, it cannot be used with AnyConnect or IPSEC - only with the Cisco ASA web login page.