CA Adapter for Juniper SSL VPN

Configuration Guide

r2.2.9

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Performing Post-Installation Tasks

The CA Adapter for Juniper SSL VPN Configuration Guide walks you through the process to configure CA Adapter to work with the Juniper SSL VPN appliance.

This guide requires that you be familiar with CA AuthMinder and Juniper SSL VPN appliance being used for the integration.

Note: This guide assumes that CA Adapter, Juniper SSL VPN appliance, and CA AuthMinder are installed and are independently operational.

The Adapter and Juniper SSL VPN integration enables VPN users to leverage CA's unique software-based credential, CA ArcotID PKI, to provide authenticated access to the network resources.

After installing and configuring Adapter 2.2.9, you must configure CA AuthMinder to communicate with the Juniper SSL VPN appliance. This chapter describes how you can configure CA AuthMinder and Juniper SSL VPN appliance to integrate with your primary authentication mechanism.

This chapter covers the following topics:

Before proceeding with the instructions given in this chapter, ensure that Adapter is installed and configured. For information on installing and configuring Adapter, see the *CA Adapter Installation and Configuration Guide*.

Note: CA Adapter still contains the terms Arcot, RiskFort and WebFort in some of its code objects and other artifacts. Therefore, you will find occurrences of Arcot, RiskFort and WebFort in all CA Adapter documentation. In addition, some of the topics in this guide do not follow the standard formatting guidelines. These inconsistencies will be fixed in a future release.

Configuring AuthMinder

Perform the following tasks to configure RADIUS protocol support in AuthMinder:

1. Enabling RADIUS Protocol Support in AuthMinder Server.
2. Create RADIUS clients.

Note: For complete information about working with the RADIUS protocol in AuthMinder, see the *CA AuthMinder Installation and Deployment Guide*.

Enabling RADIUS Protocol Support in AuthMinder Server

You must use the AuthMinder Administration Console to enable RADIUS protocol support. You must do this after you have successfully configured AuthMinder Server and the AuthMinder Administration Console.

To enable RADIUS protocol support in AuthMinder Server:

1. Log in to AuthMinder Administration Console as *Master Administrator* by using the following URL:

   http://*host_name*:*port_number*/arcotadmin/masteradminlogin.htm

   In the preceding URL, *host_name* indicates the host name or the IP address of the application server where you configured Administration Console and *port_number* indicates the port at which the server listens to incoming requests.
2. Click the Services and Server Configurations tab.
3. Activate the WebFort tab.
4. Under Instance Configurations in the side-bar menu, click Protocol Management.

   The Protocol Configuration page opens.
5. In the List of Protocols table, click RADIUS.

   The RADIUS page opens.
6. Select the Change Protocol Status check box.
7. From the Action drop-down list, select Enable.
8. Click Save to save your changes.

You have enabled RADIUS protocol support in AuthMinder Server.

Creating RADIUS Clients

To create RADIUS clients:

1. Log in to Administration Console as *Global Administrator* by using the following URL:

   http://*host_name*:*port_number*/arcotadmin/adminlogin.htm

   In the preceding URL, *host_name* indicates the host name or the IP address of the application server where you configured Administration Console and *port_number* indicates the port at which the server listens to incoming requests.

2. Click the Services and Server Configurations tab.
3. Activate the WebFort tab.
4. In the left pane, click RADIUS Client.

   The RADIUS Configuration page opens.

5. Click Add.

   The page to add a new RADIUS Configuration page opens.

6. Provide information to add a new RADIUS configuration, as described in the following table.

Parameter	**Description**
RADIUS Client IP Address	The IP Address of the RADIUS client, which is the Juniper Secure Access gateway IP.
Shared Secret Key	The secret key that is shared between the RADIUS client and AuthMinder Server. **Note:** The minimum length of the key is 1 and the maximum length is 512 characters.
Description	A brief description of the RADIUS client. The description helps identify the RADIUS client, when multiple clients are configured.
Authentication Type	Select **RADIUS OTP** as the type of authentication that is used with VPNs.

7. Click the Add button to add the IP address of the new RADIUS client.

   Note: The RADIUS Configuration page also displays the Existing RADIUS Clients table, using which you can update or delete the RADIUS client IP addresses.

8. Restart the AuthMinder Server.

You have created an AuthMinder RADIUS client.

Configuring Juniper SSL VPN

You must configure the Juniper SSL VPN appliance after you have successfully configured the RADIUS protocol support and added a RADIUS client in AuthMinder.

To configure the Juniper SSL VPN appliance:

1. Log in to Juniper SSL VPN Administration Console.

   The login screen of the Juniper SSL VPN Administration Console opens.

   On successful authentication, the Juniper SSL VPN appliance grants access to the user.

2. Add an authentication server for the RADIUS-based authentication, as follows:

   a. In the left pane, click Auth Servers in the Authentication section.

      The Authentication Servers page opens.

   b. From the New drop-down list, select Radius Server and then click New Server.

      The New Radius Server page opens.

   c. Use the information provided in the following table to enter the fields in the first section of this page.

Field Name	**Required/ Optional**	**Description**
Name	Required	Specify a name for the RADIUS Server.
NAS-Identifier	Optional, *if* NAS-IP-Address is specified	Specify the Fully Qualified Distinguished Name (FQDN) of the client to identify itself to the RADIUS server.
Radius Server	Required	Specify the FQDN or IP address of RADIUS Server.
Authentication Port	Required	Specify the port at which RADIUS Server is available. Default value: 1812
Shared Secret	Required	The shared secret that you specify here must match the Shared Secret Key value that you specified on the RADIUS Configuration page while configuring AuthMinder.
Accounting Port	Required	Specify the port at which the RADIUS accounting service is available. Default value: 1813

Field Name	Required/ Optional	Description
NAS-IP-Address	Optional, *if* NAS-Identifier is specified	Specify the IP address of the client to identify itself to the RADIUS server.
Timeout	Required	Specify the time (in seconds) before the system times out.
Retries	Required	Specify the number of times a user is allowed to try to authenticate.

d. Select the Users authenticate using tokens or one-time passwords check box.

e. Similarly, refer to the preceding table to specify information for the Backup server section.

f. (Optional) Specify the information in the Radius accounting section, if you are using an authorization server.

g. (Optional) Specify the information in the Custom Radius Rules section, if required.

h. Click Save Changes to add the new server to the list.

3. Define a user realm for the new authentication server that you added in Step 2.

   a. In the Users section, point to User Realms, and then click New User Realm.

      The New Authentication Realm page opens.

   b. On the New Authentication Realm page, enter the following information:

      - Name: Enter the name of the new realm that you are creating.

      Note: Ensure that the realm name you specify clearly describes the user community so that users can identify the realm correctly.

      - Description: Enter a description for the realm.
      - Authentication: Select the authentication server that you added in Step 2 from the list.
      - Accounting: Select None from the drop-down list.

   c. Click Save Changes to add the new realm.

4. Define a role mapping rule for the realm that you created in Step 3.

   a. In the Users section, point to User Realms, point to the realm created in Step 3, and then click Role Mapping.

      The Role Mapping Rule page opens.

   b. Click New Rule.

      The new Role Mapping Rule page opens.

   c. On the Role Mapping Rule page, enter the following information:

      - Rule based on: Select Username from the drop-down list.
      - Name: Enter the name of the new rule that you are creating.
      - Rule: If username: Select is from the drop-down list and enter * in the text box, which indicates that rule will be applied to all users.
      - To assign this rule to a role, select the role in the Available Roles list and click the Add button to add the selected role to the Selected Roles list. For example, add Users role to the Selected Roles list.

   d. Click Save Changes to add the new role mapping rule.

5. Change the user's network connect client type.

a. In the Users section, point to User Roles, and then click Users (the role selected in substep c in the preceding step).

   The Users role page opens.

b. Under Network Connect, select the Network Connect option.

c. Click Save Changes to change the network connect client type.

6. Upload custom sign-in pages.

   a. In the Authentication section, point to Signing In, and then click Sign-in Pages.

      The Signing In page opens.

   b. Click Upload Custom Pages.

      The Upload Custom Sign-In Pages screen opens.

   c. In the right pane, under the Sample Template Files section, click Sample to download the Sample.zip file.

   d. Extract the contents of the sample.zip file.

   e. Locate the LoginPage.thtml file shipped with the sample application, and open it in a text editor.

   f. Locate the JavaScript function deletepreauth() and include the following code before the ending script tag (/script):

```
function delegateAuthentication(){
var toberemoved = document.getElementsByTagName("input");
var loginAction = document.frmLogin.action;
var browserUrl = window.location;
for (var i=0; i < toberemoved.length; i++) {
var name = toberemoved[i].getAttribute("name");
if (name == "username") {
var parentNode = toberemoved[i].parentNode;
parentNode.removeChild(toberemoved[i]);
}
}
document.getElementById("posturl").value = loginAction;
document.getElementById("browserurl").value = browserUrl;
document.frmLogin.action =
"https://host_name:port/arcotafm/master.jsp?profile=arcotidrisk";
document.frmLogin.submit();
}
```

      Note: In the preceding code, replace *hostname* and *port* with the host name and port of the server hosting Authentication Flow Manager (arcotafm). In addition, *arcotidrisk* represents the AFM profile created by using the Wizard and supports SSL VPN integration.

   g. Replace the code within the <form> and </form> tags with the following code:

Note: In the following code, replace the form's action parameter with the complete URL of the login.cgi file hosted on the Juniper SSL VPN appliance. Contact Juniper SSL VPN administrator to get the complete URL assigned to the login.cgi page.

```
<form name="frmLogin" action=login.cgi method="POST" autocomplete=off
onsubmit="return Login(<% setcookies %>)">
<input type="hidden" name="tz_offset">
<input type="hidden" name="vpn" value="true">
<input type="hidden" name="type" value="juniper_lite">
<input id="posturl" type="hidden" name="posturl" value="">
<input id="browserurl" type="hidden" name="browserurl" value="">
<input id="errormessage" type="hidden" name="errormessage" value="<%
LoginPageErrorMessage %>">
<table border="0" cellpadding="2" cellspacing="0">
<tr>
<td nowrap colspan="3"><b><% welcome FILTER verbatim %></b></td>
</tr>
<tr>
<td nowrap colspan="3"><span class="cssLarge"><b><% portal FILTER
verbatim %></b></span></td></tr>
<tr>
<td colspan="3"> </td>
</tr>
<% IF LoginPageErrorMessage %>
<tr>
<td colspan=3>
<table cellpadding=1 bgcolor=#cccc99><tr>[assign the value for TD in your
book]
<table cellpadding=2 bgcolor=#FFFFCC><tr>[assign the value for TD in your
book]
<% LoginPageErrorMessage %>
</td></tr></table>
</td></tr></table>
</td>
</tr>
<% END %>
<tr>
<td valign="top">
<table border="0" cellspacing="0" cellpadding="2">
<%IF !AnonymousAuthentication && !CertificateAuthentication &&
!SAMLAuthentication%>
<% FOREACH prompt = prompts %>
<%NEXT IF !prompt.required %>
<% END %>
<tr>

<% IF RealmList.size == 0 %>
[assign the value for TD in your book]<% realm %></td>[assign the value for
TD in your book] </td>[assign the value for TD in your book]
```

```
<input type="text" name="realm" value="" size="20">
</td>
<% ELSIF RealmList.size == 1 %>
<input type="hidden" name="realm" value="<% RealmList.0 %>">
<script type="text/javascript">
delegateAuthentication();
</script>
<% ELSE %>
[assign the value for TD in your book]<% realm %></td>[assign the value for
TD in your book] </td>[assign the value for TD in your book]
<select size="1" name="realm">
<% FOREACH r = RealmList %>
<option value="<% r %>" ><% r %></option>
<% END %>
</select>
</td>
<% END %>
</tr>
<%ELSE%>
<tr>
<input type="hidden" name="realm" value="<% RealmList.0 %>">
<script type="text/javascript">
delegateAuthentication();
</script>
</tr>
<%END%>
<tr>
<td colspan="3"> </td>
</tr>
<tr>
[assign the value for TD in your book] </td>
[assign the value for TD in your book] </td>
[assign the value for TD in your book]<input type="button" value="Continue"
name="btnSubmit"
onclick="javascript: delegateAuthentication()"> 
<% IF help_on %>
<input type='submit' name='help' value="<% help %>"
onclick='window.open("welcome.cgi?p=help", "wndHelp",
"height=400,width=500,resizeable=yes,scrollbars=yes"); return false;'>
<% END %>
</td>
</tr>
<% IF admin %>
<tr>
<td colspan="3"> </td>

</tr>
<tr>
<td colspan="3" align="center">
```

```
<table border="0" cellspacing="0" cellpadding="1" width="220">
<tr>
<td width="220" bgcolor="#CCCC99">
<table border="0" cellpadding="2" cellspacing="0" width="220">
<tr>
<td bgcolor="#FFFFCC">Note: This is the <br><b>Administrator Sign-In
Page</b>.
<br><br>If you don't want to sign in as an Administrator, return to the
<a href="<% enduserSigninURL %>">standard Sign-In Page</a>.
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
<% END %>
</table>
</td>
<td valign="top">      </td>
<td valign="top"><TABLE border="0" cellspacing="0" cellpadding="2">
<tr>[assign the value for TD in your book]Please select a Realm and
continue</tr></td></table></td>
</tr>
</table> </form>
```

h. Save and close the LoginPage.thtml file.

i. Update the LoginPage.thtml file in Sample.zip with the LoginPage.thtml file that you edited in the preceding step.

j. On the Upload Custom Sign-In Pages screen, enter the name (for example, Adapter Sign-in Page) that you will use to reference the custom sign-in pages in the Name field.

k. In the Templates File field, click Browse to navigate to the location of custom templates (updated Sample.zip, see step i above).

l. Click Upload Custom Pages to use the sign-in page provided by CA.

The "Successfully created new Custom Sign-In page." message opens.

7. Define a user URL that would be used for authentication.

a. In the Authentication section, point to Signing In, and then click Sign-in Policies.

The Signing In page opens.

b. Click New URL.

The New Sign-in Policy page opens.

c. On the New Sign-in Policy page, specify the following information:

- User type: Select Users.

- Sign-in URL: Specify the URL that will be used to access the custom login page that you created. For example, specify the afmlogin URL.
- Sign-in page: Select the Sign-in page that you created (AFM Sign-in Page).

d. In the Authentication realm section, specify the following:

- Select User picks from a list of authentication realms to allow the user to select the realm to log in.
- Select the realm that you created in the Available realms list and click Add to add the selected realm to the Selected realms list.

e. Click Save Changes to save the changes you made.

Verifying Juniper SSL VPN Integration

To test the Juniper VPN integration:

1. Restart the application server where AFM is installed.
2. From the end-user's system, launch a new instance of the Web browser and access the URL configured for VPN, as shown:

   http[s]://*host_name*/*sign_in_URL*

   In the preceding URL syntax, *host_name* points to the VPN to which you redirected the user requests and *sign_in_URL* points to the URL that you configured for the Arcot realm, which is afmlogin. You should see the AFM login page.

If you see the AFM page, it indicates that you have successfully configured Adapter with Juniper SSL VPN.

Chapter 1: Performing Post-Installation Tasks 5