F5 APM Integration

Contents

- 1 F5 Big-IP Access Policy Manager (APM) Integration Notes
- 2 RADIUS Integration
    - 2.1 Test the RADIUS authentication
- 3 Logon page Customisation
    - 3.1 Removing the Automatic TURing image
- 4 Testing

F5 Big-IP Access Policy Manager (APM) Integration Notes

This article describes how to integrate the F5 Big-IP Access Policy Manager with Swivel. The article covers two aspects:

- the integration of the two servers so that the F5 uses Swivel as its RADIUS server
- the modification of the F5 login page to include the TURing image or other Swivel elements as required.

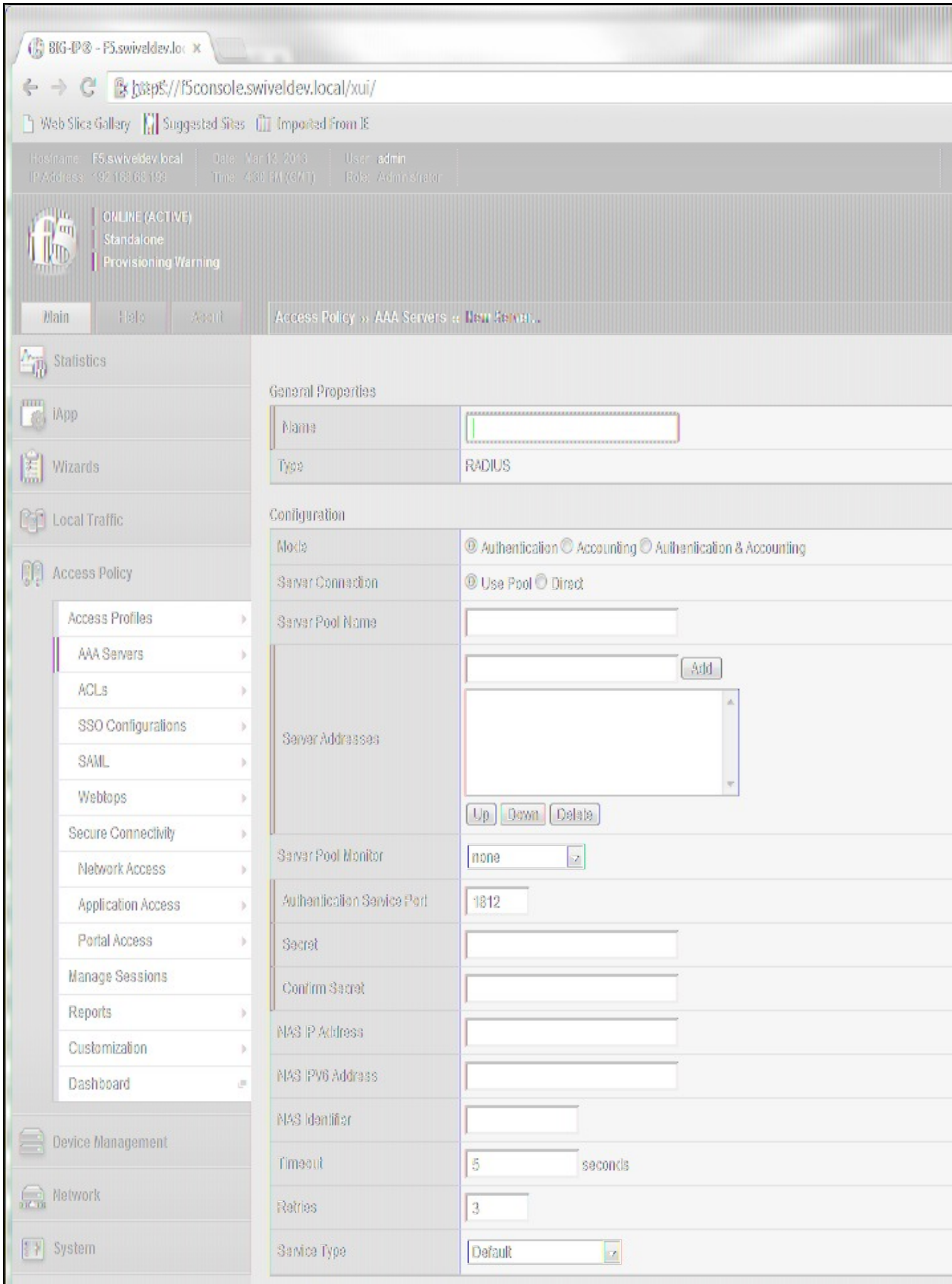
RADIUS Integration

To use Swivel with F5 Big-IP you need to enable the Radius Server on Swivel. (On the RADIUS->Server page)

A NAS Entry then need to be created that includes the F5 server IP address/hostname and a shared secret.

The associated configuration then needs to be created on the F5 server.

This is done on the Access-Policy->AAA-Servers screen.


BIG-IP® - F5.swiveldev.loc
https://f5console.swiveldev.local/xui/
Web Slice Gallery
Suggested Sites
Imported From IE
Hostname: F5.swiveldev.local
IP Address: 192.168.66.199
Date: Mar 13, 2013
Time: 4:30 PM (GMT)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Provisioning Warning
Main
Help
Acout
Access Policy » AAA Servers « New Server...
Statistics
iApp
Wizards
Local Traffic
Access Policy
Access Profiles
AAA Servers
ACLs
SSO Configurations
SAML
Webtops
Secure Connectivity
Network Access
Application Access
Portal Access
Manage Sessions
Reports
Customization
Dashboard
Device Management
Network
System
General Properties
Name
Type
RADIUS
Configuration
Mode
Authentication
Accounting
Authentication & Accounting
Server Connection
Use Pool
Direct
Server Pool Name
Server Addresses
Add
Up
Down
Delete
Server Pool Monitor
none
Authentication Service Port
1812
Secret
Confirm Secret
NAS IP Address
NAS IPV6 Address
NAS Identifier
Timeout
5
seconds
Retries
3
Service Type
Default

Once this entry has been created it can be used when defining Access Profiles.

It is important to remember the name of the profile created as this will be required for the customisation.

Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

Logon page Customisation

Once you have configured your access policy, you need to modify the logon page. You can edit it from the management console as follows:

From the Main menu, select Access Policy, then Customization. From the View dropdown, select Advanced Customization. From the folder tree, select Customization Settings -> Access Profiles -> [Your access profile] -> Access Policy -> Logon Pages -> Logon Page -> logon.inc.

Search for the line

```
function OnLoad()
```

Insert the following immediately before it:

For TURing image:

```
// **** PINsafe Customisation Start ****

// Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCImage?username=";

function ShowTuring() {
  var usernameField = document.getElementById("input_1");
  if (usernameField && usernameField.value && usernameField.value != "") {
    var img = document.getElementById("turing_img");
    if (img) {
      img.style.display = "";
      img.src = imageUrl + usernameField.value + "&random=" + Math.floor(Math.random()*10000);
    }
  }
}
// **** PINsafe Customisation End ****
```

Or for PinPad:

```
// **** PINsafe Customisation Start ****

// Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCPinPad?username=";

function ShowPinPad() {
  var usernameField = document.getElementById("input_1");
  if (usernameField && usernameField.value && usernameField.value != "") {
    var padno = Math.floor(Math.random() * 100000);
    for (var i=0; i<10; i++) {
      var img = document.getElementById("pinpad" + i);
      if (img) {
        var url = imageUrl + usernameField.value + "&padno=" + padno + ":" + i;
        img.src = url;
      }
    }
  }
}

function InsertPinPad() {
  var footerCell = document.getElementById("credentials_table_footer");
  if (footerCell) {
    var footerRow = footerCell.parentNode;
    var formTable = footerRow.parentNode;
    var pinpadRow = document.createElement("tr");
    pinpadRow.setAttribute("id", "turing_row");
    var pinpadCell = document.createElement("td");
    pinpadCell.setAttribute("colspan", "2");
    pinpadCell.setAttribute("align", "center");
    var pinpadTable = document.createElement("table");
    pinpadTable.style.height = "225px";
    pinpadTable.style.width = "150px";
    var row, cell, img;
    for (var r=1; r<=9; r+=3) {
      row = document.createElement("tr");
      for (var c=r; c<r+3; c++) {
        cell = document.createElement("td");
        cell.setAttribute("align", "center");
        img = document.createElement("img");
        img.src = "images/blank.png";
        img.setAttribute("id", "pinpad" + c);
        img.setAttribute("onclick", "AddDigit(" + c + ")");
        cell.appendChild(img);
        row.appendChild(cell);
      }
      pinpadTable.appendChild(row);
    }
    row = document.createElement("tr");
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
```

```
    img.src = "images/refresh.png";
    img.setAttribute("onclick", "ShowPinPad()");
    cell.appendChild(img);
    row.appendChild(cell);
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
    img.src = "images/blank.png";
    img.setAttribute("id", "pinpad0");
    img.setAttribute("onclick", "AddDigit(0)");
    cell.appendChild(img);
    row.appendChild(cell);
    cell = document.createElement("td");
    cell.setAttribute("align", "center");
    img = document.createElement("img");
    img.src = "images/clear.png";
    img.setAttribute("onclick", "ClearOtc()");
    cell.appendChild(img);
    row.appendChild(cell);
    pinpadTable.appendChild(row);
    pinpadCell.appendChild(pinpadTable);
    pinpadRow.appendChild(pinpadCell);
    formTable.insertBefore(pinpadRow, footerRow);
  }
}

// Check that the following field is correct. If PINsafe is the ONLY form of authentication,
// or is the first authentication, it will be "input_2".
// If it is the second authentication, it will be "input_3".
var otcFieldId = "input_2";

function AddDigit(digit) {
  var otcField = document.getElementById(otcFieldId);
  if (otcField) {
    otcField.value += digit;
  }
}

function ClearOtc() {
  var otcField = document.getElementById(otcFieldId);
  if (otcField) {
    otcField.value = "";
  }
}

// **** PINsafe Customisation End ****
```

A few lines below this are the following lines:

```
if( form == null ){
  return;
}
```

Below this, insert the following for TURing:

```
// **** PINsafe Customisation Start ****
var footerCell = document.getElementById("credentials_table_footer");
if (footerCell) {
  var footerRow = footerCell.parentNode;
  var formTable = footerRow.parentNode;
  var turingRow = document.createElement("tr");
  turingRow.setAttribute("id", "turing_row");
  var turingCell = document.createElement("td");
  turingCell.setAttribute("colspan", "2");
  turingCell.setAttribute("align", "center");
  var turingImg = document.createElement("img");
  turingImg.setAttribute("id", "turing_img");
  turingImg.style.display = "none";
  turingCell.appendChild(turingImg);
  var turingBrk = document.createElement("br");
  turingCell.appendChild(turingBrk);
  var turingBtn = document.createElement("input");
  turingBtn.setAttribute("type", "button");
  turingBtn.setAttribute("value", "New Image");
  turingBtn.onclick = ShowTuring;
  turingCell.appendChild(turingBtn);
  turingRow.appendChild(turingCell);
  formTable.insertBefore(turingRow, footerRow);
}
// Optional: to automatically show the TURing after entering the username, include the following lines.
var usernameField = document.getElementById("input_1");
if (usernameField) {
  usernameField.onblur = ShowTuring;
}
// Optional: if the username is pre-populated, use the following line to display the TURing image immediately
ShowTuring();
// **** PINsafe Customisation End ****
```

or this for Pinpad:

```
  // **** PINsafe Customisation Start ****
  InsertPinPad();
  // The next section is optional - use this if you want to show the TURing automatically when the username changes.
  var usernameField = document.getElementById("input_1");
  if (usernameField) {
    usernameField.onblur = ShowPinPad;
  }
  // **** PINsafe Customisation End ****
```

Removing the Automatic TURing image

Remove or comment out the following lines with // at the front

```
// Optional: to automatically show the TURing after entering the username, include the following lines.
var usernameField = document.getElementById("input_1");
if (usernameField) {
  usernameField.onblur = ShowTuring;
}
```

For Pinpad, the penultimate line above will be

```
  usernameField.onblur = ShowPinPad;
```

The final step here is to set the image URL. There are a number of options:

- The simplest option is to use the Swivel Server directly. However, this requires that the Swivel Server is directly accessible from the internet, which is not a recommended solution, as it is a security risk. Also, you will need a commercial SSL certificate on the Swivel server to avoid problems with certificate errors. In this case, simply replace *<your_swivel_server>* above with the external URL of your Swivel Server.
- The second option is to create a virtual server on the F5 Big-IP to act as an anonymous proxy to the Swivel Server. This is suitable if the F5 is your only Swivel integration, as it requires that the F5 is set as the default gateway for your Swivel appliance. Details for this are not provided, as it should be clear from the F5 documentation how to do this. You might also want to create an iRule to restrict access only to the TURing image, as suggested below. In this case, you should replace *<your_swivel_server>* with the external URL of your F5. If you have set up the virtual server with a different service port, you might need to change this as well.

```
when HTTP_REQUEST {
  if { [HTTP::uri] starts_with "/pinsafe/SCImage?" } {
    pool PINsafe_8080
  } else { HTTP::respond 403 }
}
```

- The third option is suitable if you have other Swivel integrations. In this case, you can use the URL of the TURing image on the other integration to deliver the TURing image. For example, if you have an integration with Outlook Web Access, use the following:

```
var imageUrl = "https://<your_swivel_server>/owa/auth/SCImage.aspx?username=";
```

Here, replace *<your_swivel_server>* with the URL of your OWA server.

Another example: if you have a UAG integration, use the following:

```
var imageUrl = "https://<your_swivel_server>/InternalSite/images/customupdate/images.asp?username=";
```

NOTE: If you are using Pinpad, substitute **SCPinPad** for **SCImage** above.

Testing

Now when the F5 server is accessed via the **pinsafe** access policy the user should see a modified login page with the option to request a TURing image.

The user should enter their username and see a TURing image when the click the TURing button. At this point a Session Start message for the user should show in the PINsafe logs.

If no image shows, check that the URL is correct and ensure that there is no firewalls blocking the request.

Also check that Session Create by Username is enabled on the Swivel server.

The user should then enter their one-time code. The login.

If the log-in fails, check the Swivel log files to see if a RADIUS request was logged. If not then check the settings for the RADIUS on F5 and Swivel to ensure IP Addresses, port numbers and shared secrets all match. Also check that no firewalls are blocking the RADIUS requests.

If RADIUS attempts are being logged but authentication is failing, check that the session was started correctly and that there is no password associated with the account etc.