Mobile ID
F5 Access Policy Manager

Solution guide

Version: 1.0

Swisscom (Schweiz) AG
Security Solutions

Swisscom (Schweiz) AG
Security Solutions

Contents

1 Introduction

The purpose of this document is to provide clarifications **how** to interface Mobile ID with F5 Access Policy Manager (BIG-IP) to authenticate a user with Mobile ID while requesting access to applications and network through BIG-IP.

This manual assumes that you are familiar with BIG-IP and Swisscom Mobile ID.

More details about Mobile ID can be found in the Mobile ID SOAP client reference guide [1].

Terms and abbreviations

Abbreviation	Definition
	Please note:
	Be careful, important:
AP	Application Provider
DataToBeDisplayed DTBD	Data to be displayed
DataToBeSigned DTBS	Data to be signed
MSSP	Mobile Signature Service Provider
M-ID or MID	Mobile ID platform providing the mobile signature service
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network
SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of Web Services relying on Extensible Markup Language (XML)
WS	A Web service (WS) is a method of communication between two electronic devices over the Web (Internet).

1.1 Referenced documents

[1] SOAP Client Reference Guide
[2] RADIUS Integration Guide
[3] SAML and SuisseID Integration Guide
[4] BIG-IP Access Policy Manager Authentication Configuration Guide: RADIUS Authentication
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-11-5-0/7.html
[5] BIG-IP Access Policy Manager: SAML Configuration Guide
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-11-5-0/27.html#conceptid
[6] Using APM as a SAML Service Provider
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-11-5-0/30.html
[7] BIG-IP Access Policy Manager: Implementations: Configuring APM for web access management
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-implementations-11-5-0/1.html

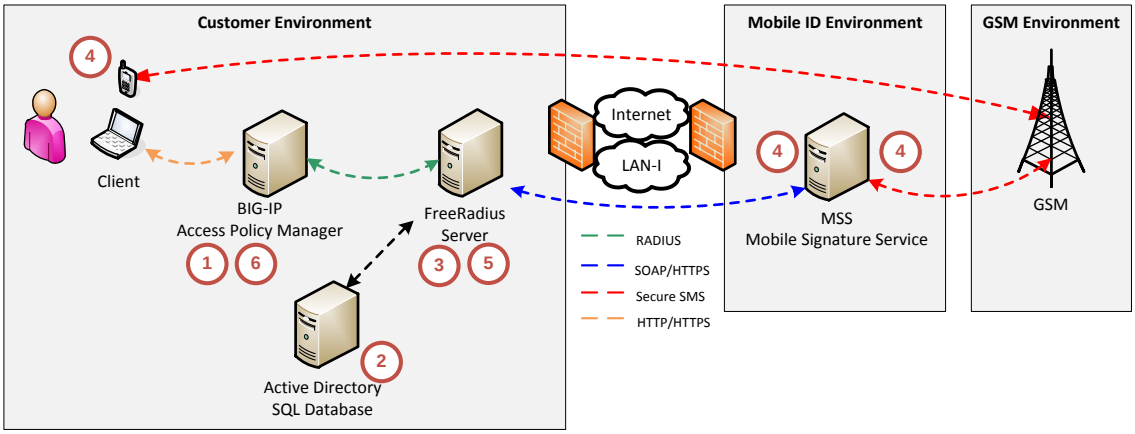
2 Overview and main scenario

This chapter describes a possible solution to interface the Access Policy Manager (BIG-IP) with Mobile ID.

The solution detailed in this guide is based on the available Radius interface at the BIG-IP side. This interface communicates with a RADIUS server, in our case an on premise FreeRADIUS server. Basically it can be done with any RADIUS server that is extensible and would allow the integration of the Mobile ID. Such a Mobile ID integrated server based on FreeRADIUS has been documented in [2].

Scenario - Strong Authentication with BIG-IP:

Before entering into more technical details, let's have a short look at the main solution:



This picture shows a user who request access to the applications or the network via BIG-IP. BIG-IP then sends the RADIUS requests to the FreeRADIUS server to authenticate the user. FreeRADIUS will invoke the Swisscom Mobile ID service over SOAP and provide the answer back to the RADIUS client interface of BIG-IP. FreeRADIUS server may also be connected to an external user store, like Microsoft Active Directory, where the end users details like phone number or credentials are stored.

Here the authentication dataflow:

1. When a user tries to access the applications or the network, BIG-IP makes a request to the defined FreeRADIUS server to authenticate the end user with Mobile ID.
2. FreeRADIUS server, optionally, verifies the user credentials against internal user stores and/or maps to a valid mobile phone user
3. FreeRADIUS server (which enabled the Mobile ID plugin) calls the Mobile ID service
4. The Mobile ID platform ensures that the end-user signature request is allowed and forwards the signature request to the end-user's mobile phone
5. The end-user answer will be processed by the Mobile ID platform and provided to FreeRADIUS server
6. After verification of Mobile ID response by FreeRADIUS server, the answer will be forwarded to BIG-IP (over its RADIUS client interface). This answer will be processed by the Access Policy Manager to grant or reject the requests.

3 Configuration and Best Practices

In this reference guide we assume that:

1. The preconditions defined in [1] are met.
2. The customer has built an intermediate protocol gateway like the FreeRADIUS server described in [2] (with the Mobile ID plugin).

3.1 Configuration of freeRADIUS in the Access Profile on BIG IP

To use the AAA RADIUS Server an Access Policy must be defined, in its simplest form this would be an LTM-APM policy attached directly to a virtual server definition. The configuration of BIG-IP must be performed as described by F5 in [7].

A simple Access Policy can be defined as follow:

1. Profile type 'LTM-APM' with parent profile 'access'
2. Optional Logout URI(s) defined.
3. Accepted Languages as appropriate.

General Properties

Name	ap-mobileid-test
Partition / Path	Common
Parent Profile	access
Profile Type	LTM-APM

Settings Custom ☐

Inactivity Timeout	900 seconds	☐
Access Policy Timeout	300 seconds	☐
Maximum Session Timeout	0 seconds	☐
Minimum Authentication Failure Delay	2 seconds	☐
Maximum Authentication Failure Delay	5 seconds	☐
Max Concurrent Users	0	☐
Max Sessions Per User	0	☐
Max In Progress Sessions Per Client IP	0	☐
Restrict to Single Client IP	☐	☐

Configurations

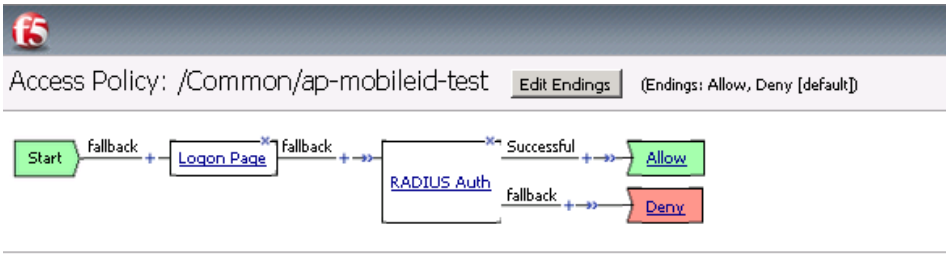
Logout URI Include	URI [Add] /logout /logout.html [Edit] [Delete]
Logout URI Timeout	5 seconds
Microsoft Exchange	None
User Identification Method	HTTP

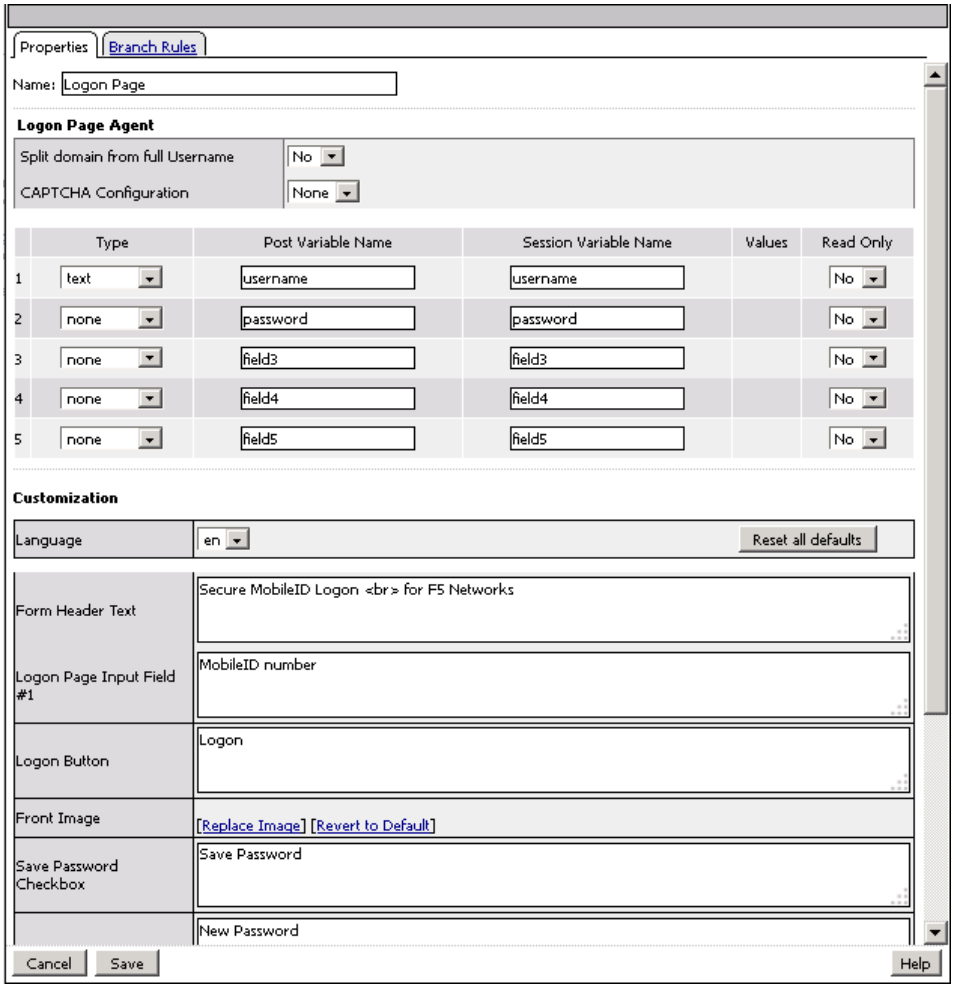
Language Settings

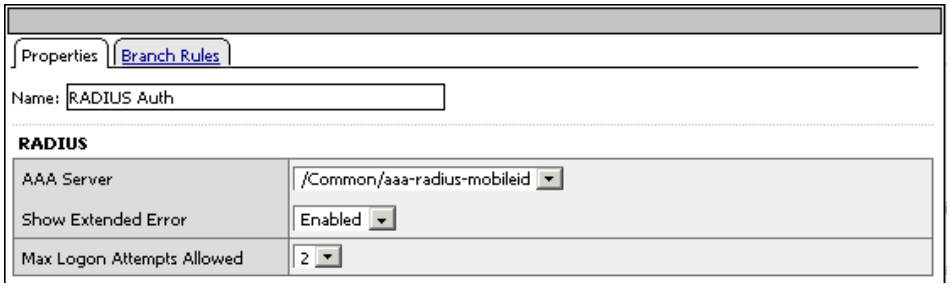
Additional Languages	Afar (aa) [Add]
Languages	Accepted Languages: English (en) Factory Builtin Languages: Japanese (ja), Chinese (Simplified) (zh-cn), Chinese (Traditional) (zh-tw), Korean (ko), Spanish (es), French (fr), German (de) [<<] [>>]
Default Language	English (en)

[Update] [Delete...]

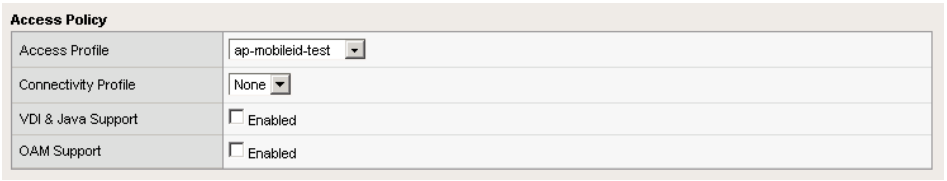
4. A simple Access Policy design with a straight forward logon page







5. Basic virtual server assignment.



6. Test access using the mobile phone number as the 'Username' on the logon page.

3.2 Configuration of FreeRADIUS as a AAA server on BIG IP

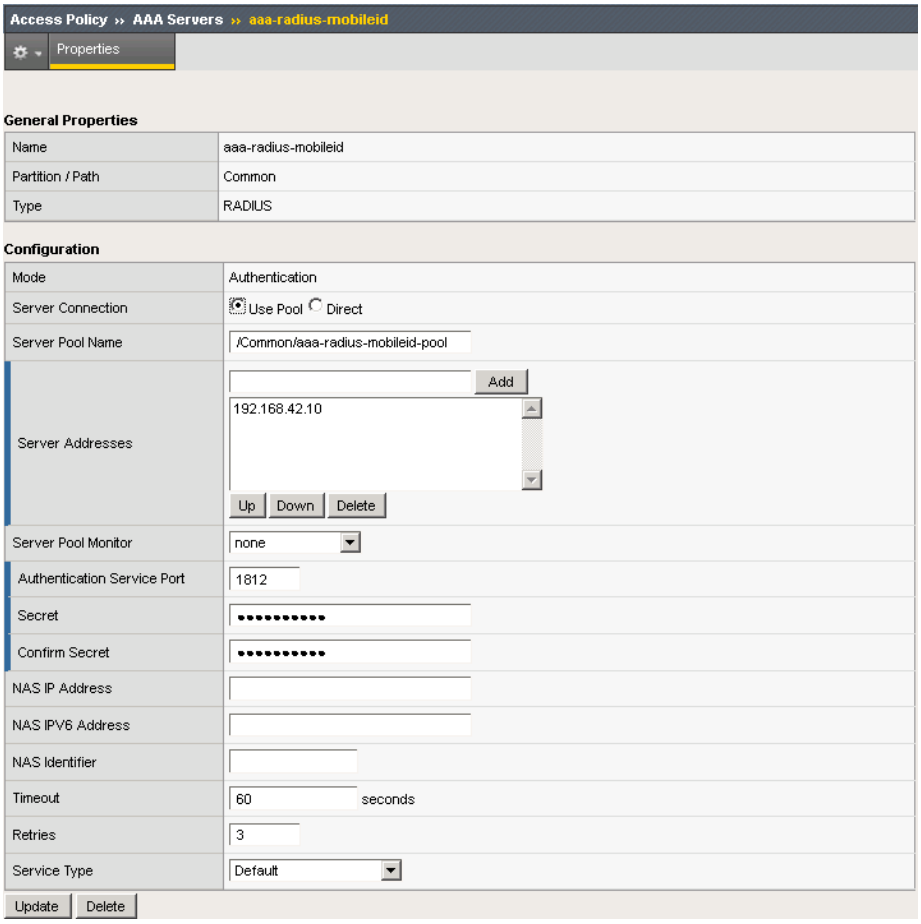
To allow BIG-IP to perform a Mobile ID authentication, the Access Policy Manager (APM) must be configured to reroute the user requests towards the FreeRADIUS server. The configuration of BIG-IP must be performed as described by F5 in [4].

N.B. Before you set up a RADIUS access policy to complete the authentication process, you must have at least one RADIUS authentication server configured (see section 2)

Basically, the APM must define a new AAA server as such:

1. The "server address for the AAA server" is the IP address or AAA pool containing the IP addresses that refer(s) to your "on premise" FreeRADIUS server(s).
2. The "Timeout field" should be configured to 60sec in order to give enough time to Mobile ID to handle the authentication requests. Currently this is the maximum allowed in APM RADIUS AAA[1].
3. The "Secret field" is the shared secret that you defined in your "on premise" FreeRADIUS server.

   N.B. Before you set up a RADIUS access policy to complete the authentication process, you must have at least one RADIUS authentication server configured.



[1] With regards to the timeout, Swisscom has opened a case with F5 to allow a timeout up to 90 Sec.

3.3 Radius Gateway and end-users details

The document [2] describes as well how to inter-connect an external user store to the FreeRADIUS server, like Microsoft Active Directory (where the end users details like phone number or credentials are stored).

3.4 Alternative to RADIUS with SAML

As described in [5], there is not only the possibility to interface Mobile ID with the RADIUS interface of BIG-IP, but there is as well an option over SAML.

Such solution is based on the available SAML interface at BIG-IP. This interface communicates with a SAML server, in our case an "on premise" IDP server. This can be done with any SAML server that is extensible and would allow the integration of the Mobile ID. Such a Mobile ID integrated server based on the open source SAML server simpleSAMLphp has been documented in [3].

Refer to [5] and [6] to configure the Access Policy Manager as a SAML Service Provider (as a claims consumer).