

Integration of F5 BIG IP APM with DoubleClue using RADIUS

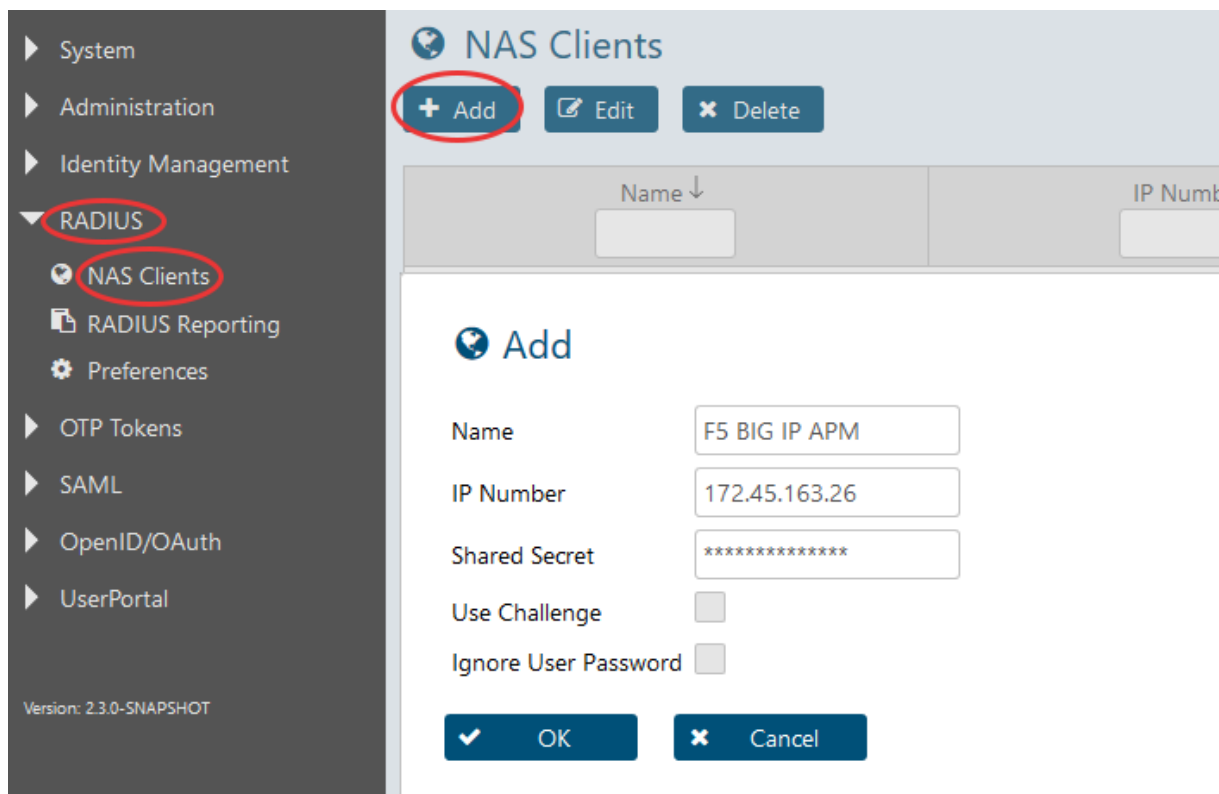


1. Introduction

This guide is intended to help administrators to use DoubleClue Multi-Factor Authentication (MFA) together with F5 BIG IP APM.

2. Preparing DCEM as a RADIUS Server

You need to add a “NAS Client” configuration in DoubleClue Enterprise Management (DCEM).



The screenshot displays the 'NAS Clients' configuration page in the DoubleClue Enterprise Management (DCEM) interface. The left sidebar shows a navigation menu with 'RADIUS' and 'NAS Clients' highlighted. The main content area shows the 'Add' form for a new NAS Client. The form includes the following fields and options:

- Name:** F5 BIG IP APM
- IP Number:** 172.45.163.26
- Shared Secret:** Masked with asterisks (*****)
- Use Challenge:**
- Ignore User Password:**

Buttons for '+ Add', 'Edit', and 'Delete' are visible at the top of the 'NAS Clients' section. At the bottom of the 'Add' form, there are 'OK' and 'Cancel' buttons.

1. In DCEM, go to main menu item "RADIUS", sub menu "NAS Clients" and click on "Add".
2. The "IP Number" must be the source IP of the F5 application.
3. Do not enable the checkboxes "Use Challenge" and "Ignore User Password".
4. Click on "OK". The configuration will be active immediately after that.

3. Configuration of F5 BIG IP APM

Here you are shown how to integrate F5 BIG IP APM with DoubleClue.

3.1 RADIUS Server Definition on the BIG-IP

The screenshot displays the F5 BIG-IP v14.0.0.1 web interface. The top navigation bar shows the user is 'admin' (Administrator) on 'Sep 27, 2018' at '12:00 PM (CEST)'. The interface is in 'ONLINE (ACTIVE) Standalone' mode. The breadcrumb trail is 'Access > Authentication > DoubleClue'. The left sidebar contains various management sections: Statistics, IApps, Wizards, Local Traffic, Traffic Intelligence, Acceleration, Access (with sub-items like Guided Configuration, Overview, Profiles / Policies, Authentication, Single Sign-On, Federation, Connectivity / VPN, Secure Web Gateway, Access Control Lists, Webtops), Device Management, Shared Objects, Network, and System. The main content area shows the 'Properties' configuration for the 'DoubleClue' RADIUS server. It is divided into 'General Properties' and 'Configuration' sections.

General Properties	
Name	DoubleClue
Partition / Path	Common
Type	RADIUS

Configuration	
Mode	Authentication
Server Connection	<input type="checkbox"/> Use Pool <input checked="" type="checkbox"/> Direct
Server Address	172.45.163.26
Authentication Service Port	1812
Secret	*****
Confirm Secret	*****
NAS IP Address	
NAS IPv6 Address	
NAS Identifier	
Timeout	60 seconds
Retries	3
Character Set	UTF-8
Service Type	Default

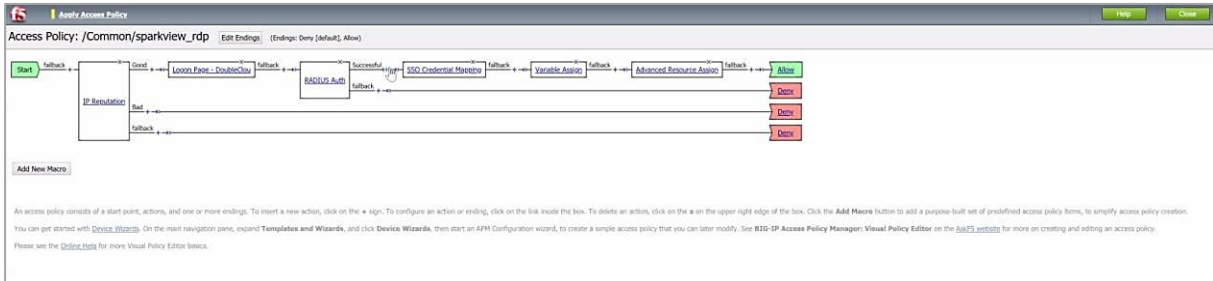
Buttons for 'Update' and 'Delete' are located at the bottom of the configuration area.

1. Go to "Main" > "Access" > "Authentication".
2. Under "Configuration", add a "Server Address", the "Authentication Service Port", a "Secret" and a "NAS IP Address".

Please note: The "Server Address" and the "NAS IP Address" must be identical with the IP address which you configured in DCEM (see previous chapter).

3. For “Timeout”, enter at least 60 seconds. However, we suggest entering 120 to 180 seconds.

3.2 Access Policy Definition



Set the Access Policy according to the screenshot above, then define the “Logon Page”, the “RADIUS Auth” and the “SSO Credential Mapping” as follows:

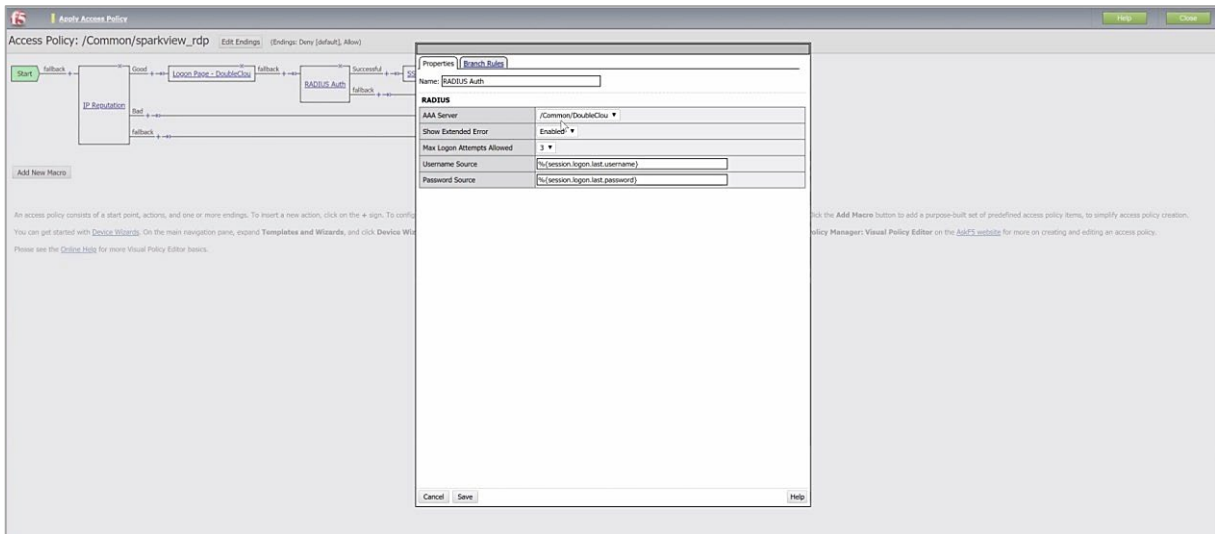
3.2.1 Logon Page Definition

Here you define the GUI of the Logon Page:

Type	Post Variable Name	Session Variable Name	Client Variable	Values	Read Only
1 text	Username	Username	No	No	No
2 password	Password	Password	No	No	No
3 none	Field3	Field3	No	No	No
4 none	Field4	Field4	No	No	No
5 none	Field5	Field5	No	No	No

3.2.2 RADIUS Server Integration

Define the RADIUS server as shown in the following screenshot. The name of the “AAA Server” must consist of the “Partition / Path” and the “Name” of the RADIUS configuration as shown in chapter 3.1.



3.2.3 SSO Credential Mapping

Here, the user credentials of RADIUS will be mapped to SSO at F5.

