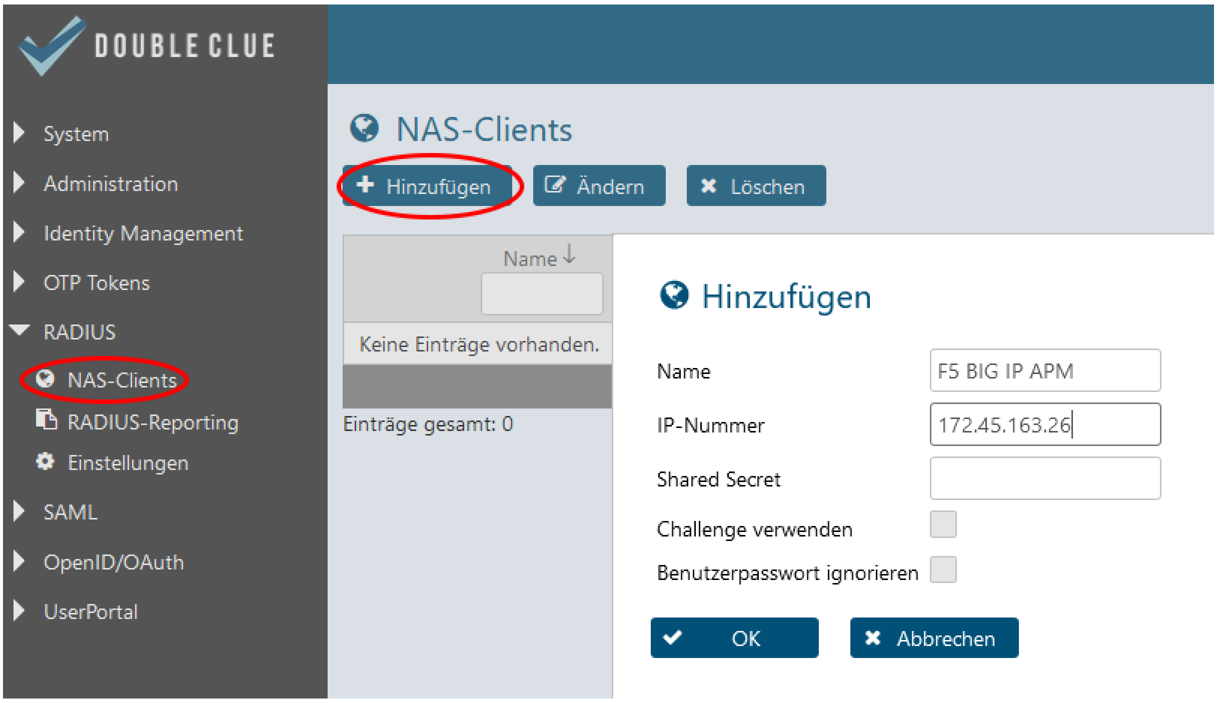
Integration von F5 BIG-IP APM mit DoubleClue via RADIUS

1. Einführung

Diese Dokumentation ist für Administratoren gedacht, welche die DoubleClue Multi-Faktor-Authentifizierung (MFA) zusammen mit F5 BIG IP APM verwenden möchten.

2. Vorbereitung von DCEM als RADIUS-Server

Sie müssen im DoubleClue Enterprise Management-System (DCEM) eine „NAS-Client"-Konfiguration hinzufügen.



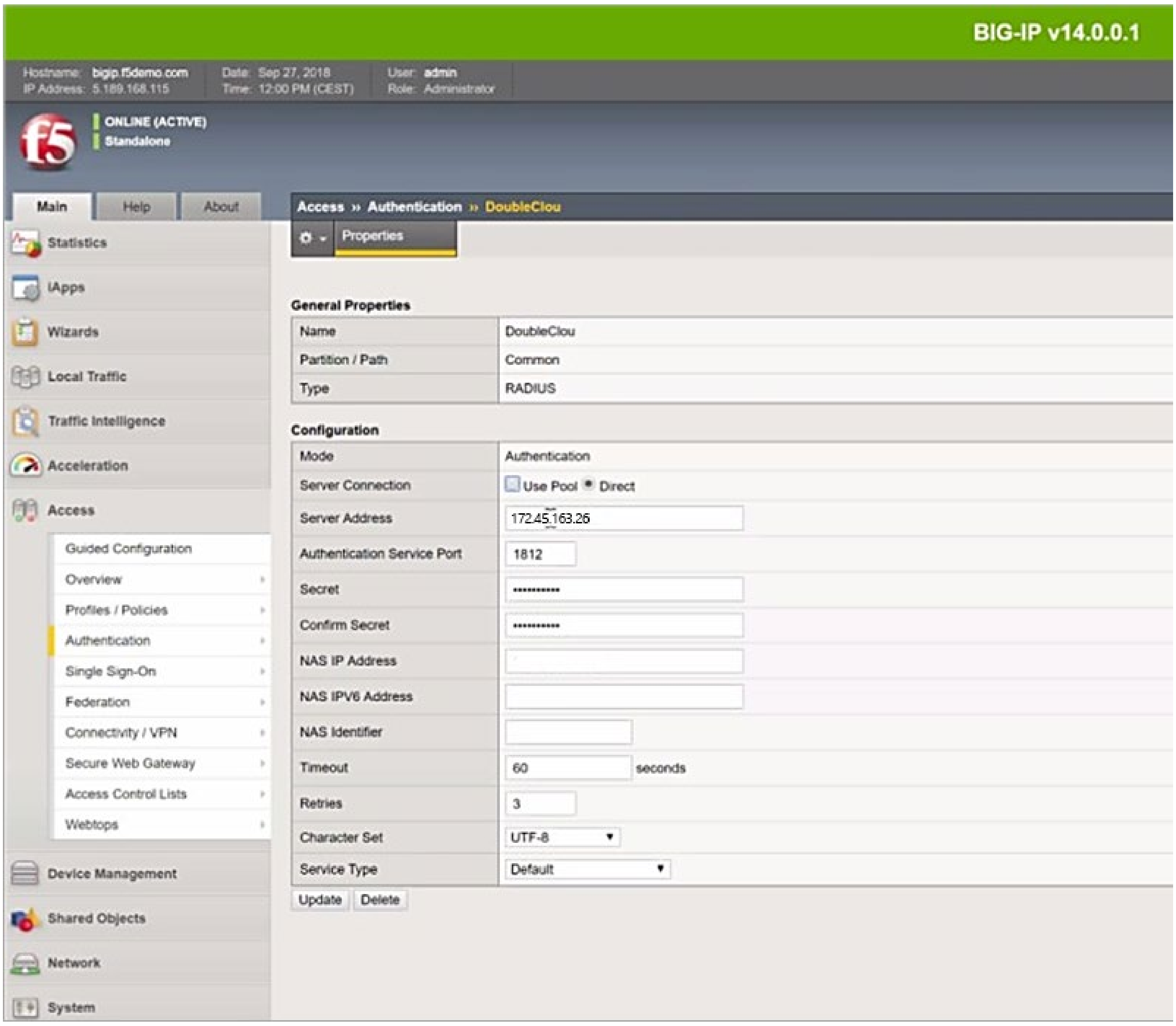
Name: F5 BIG IP APM
IP-Nummer: 172.45.163.26
Shared Secret:
Challenge verwenden ☐
Benutzerpasswort ignorieren ☐

1. Gehen Sie in DCEM zum Hauptmenüpunkt „RADIUS", Submenü „NAS-Clients", und klicken Sie auf „Hinzufügen".
2. Die „IP-Nummer" muss die Quell-IP der F5-Anwendung sein.
3. Setzen Sie in den Checkboxen „Challenge verwenden" und „Benutzerpasswort ignorieren" keinen Haken.
4. Klicken Sie auf „OK". Die Konfiguration wird sofort danach wirksam sein.

3. Konfiguration von F5 BIG-IP APM

Hier wird Ihnen gezeigt, wie Sie DCEM an F5 BIG-IP APM anbinden.

3.1 Definition des RADIUS-Servers auf der BIG-IP



General Properties

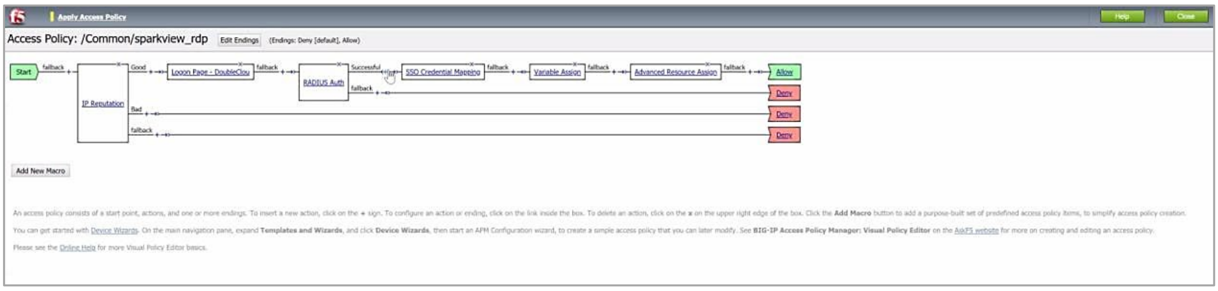
Name	DoubleClou
Partition / Path	Common
Type	RADIUS

Configuration

Mode	Authentication
Server Connection	□ Use Pool ● 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

1. Gehen Sie zu „Main“ > „Access“ > „Authentication“.
2. Fügen Sie unter „Configuration“ eine „Server Address“, den „Authentication Service Port“, das „Secret“ sowie eine „NAS IP Address“ ein.
   Bitte beachten Sie: Die „Server Address“ sowie die „NAS IP Address“ müssen identisch mit der IP-Adresse sein, welche Sie in DCEM konfiguriert haben (s. voriges Kapitel).
3. Geben Sie bei „Timeout“ mindestens 60 Sekunden ein, wir empfehlen jedoch 120 bis 180 Sekunden.

3.2 Definition der Access Policy



Access Policy: /Common/sparkview_rdp

(Endings: Deny [default], Allow)

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

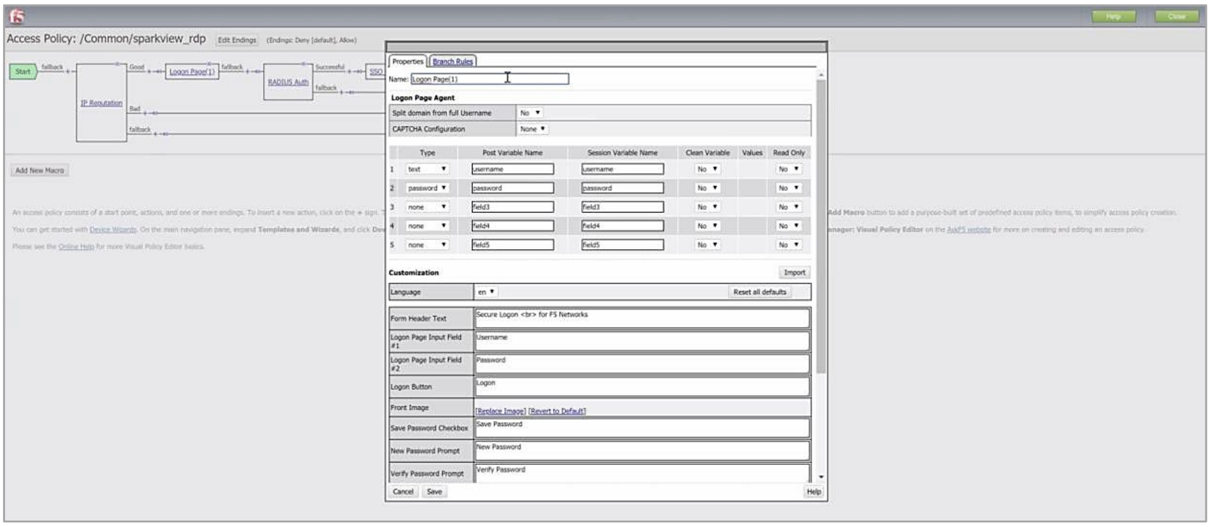
You can get started with Device Wizards. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See **BIG-IP Access Policy Manager: Visual Policy Editor** on the AskF5 website for more on creating and editing an access policy.

Please see the Online Help for more Visual Policy Editor basics.

Legen Sie die Access Policy gemäß obigem Screenshot fest und definieren Sie die „Logon Page“, die „RADIUS Auth“ sowie das „SSO Credential Mapping“ wie folgt:

3.2.1 Definition der Logon-Page

Hier legen Sie die GUI der Logon-Page fest:



Name: Logon Page(1)

Logon Page Agent

Split domain from full Username	No
CAPTCHA Configuration	None

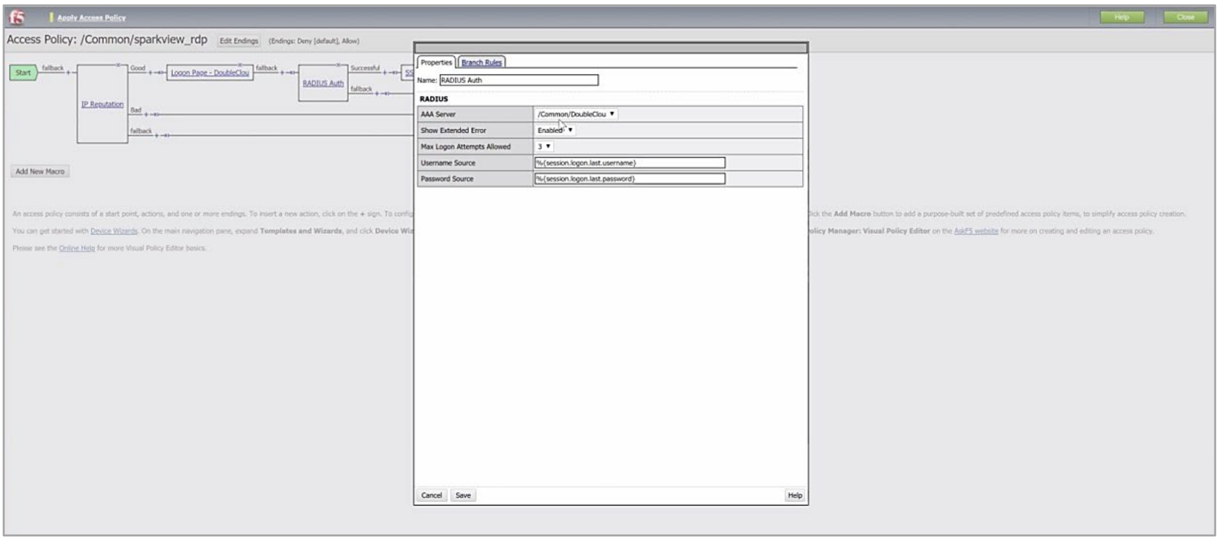
	Type	Post Variable Name	Session Variable Name	Clean Variable	Values	Read Only
1	text	username	username	No		No
2	password	password	password	No		No
3	none	field3	field3	No		No
4	none	field4	field4	No		No
5	none	field5	field5	No		No

Customization

Language	en
Form Header Text	Secure Logon for F5 Networks
Logon Page Input Field #1	Username
Logon Page Input Field #2	Password
Logon Button	Logon
Front Image	[Replace Image] [Revert to Default]
Save Password Checkbox	Save Password
New Password Prompt	New Password
Verify Password Prompt	Verify Password

3.2.2 Integration des RADIUS-Servers

Definieren Sie den RADIUS-Server wie im folgenden Screenshot gezeigt. Der Name des „AAA Server“ muss sich aus dem „Partition / Path“ sowie dem „Name“ der im Screenshot aus Kapitel 3.1 angezeigten RADIUS-Konfiguration zusammensetzen.



Access Policy: /Common/sparkview_rdp (Endings: Deny [default], Allow)

Name: RADIUS Auth

RADIUS

AAA Server	/Common/DoubleClou ▾
Show Extended Error	Enabled ▾
Max Logon Attempts Allowed	3 ▾
Username Source	%{session.logon.last.username}
Password Source	%{session.logon.last.password}

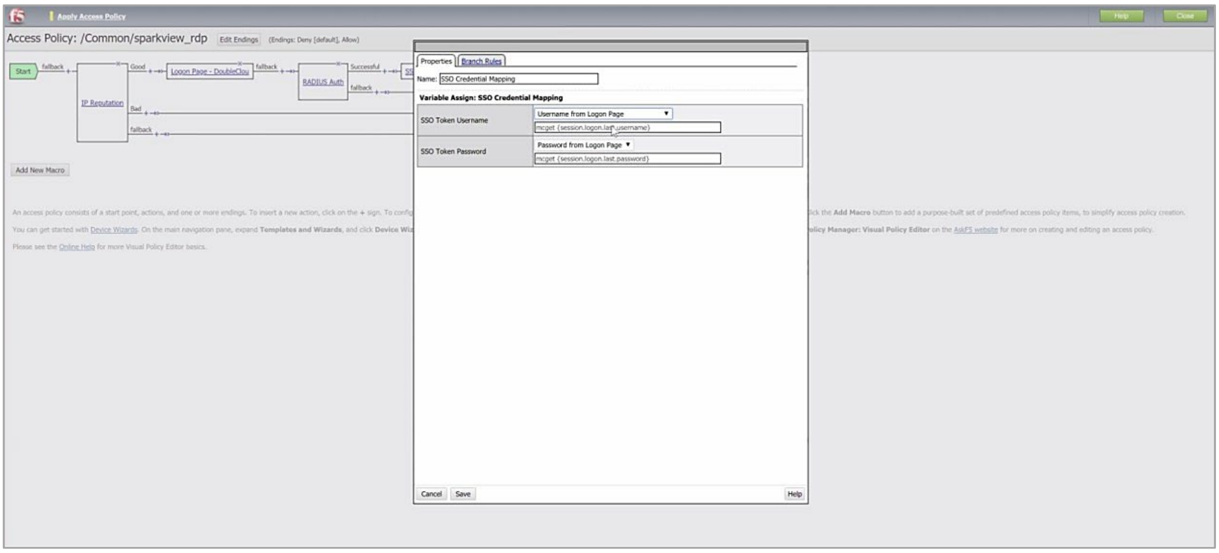
An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To config

You can get started with Device Wizards. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wiz**

Please see the Online Help for more Visual Policy Editor basics.

3.2.3 SSO Credential Mapping

Hier wird die Eingabe der Benutzer-Anmeldedaten von RADIUS an SSO gemappt.



Access Policy: /Common/sparkview_rdp (Endings: Deny [default], Allow)

Name: SSO Credential Mapping

Variable Assign: SSO Credential Mapping

SSO Token Username	Username from Logon Page ▾ mcget {session.logon.last.username}
SSO Token Password	Password from Logon Page ▾ mcget {session.logon.last.password}

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To config

You can get started with Device Wizards. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wiz**

Please see the Online Help for more Visual Policy Editor basics.