

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.

V DOUBLE CLUE					
 System Administration 	 NAS-Clients Hinzufügen Änd 	ern 🗙 Löschen			
 OTP Tokens RADIUS 	Name↓ Keine Einträge vorhanden.	Hinzufügen			
😢 NAS-Clients		Name	F5 BIG IP APM		
RADIUS-Reporting	Einträge gesamt: 0	IP-Nummer	172.45.163.26		
🌣 Einstellungen		Shared Secret			
SAML		Challenge verwenden			
OpenID/OAuth		Benutzerpasswort ignorieren			
▶ UserPortal		✓ OK 🛛 🗶 Ab	obrechen		

- 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

			BIG-IP v14.0.0.1		
Hostname: bigip.f5demo.com Date: Se IP Address: 5.189.168.115 Time: 12	p 27, 2018 User: admin :00 PM (CEST) Role: Administra				
CONLINE (ACTIVE) Standalone					
Main Help About	Access >> Authentication >>	DoubleClou			
Statistics	o - Properties				
IApps	General Properties				
Wizards	Name	DoubleClou			
RPA Local Traffic	Partition / Path	Common			
City cocal tranic	Туре	RADIUS			
Traffic Intelligence	Configuration				
Acceleration	Mode	Authentication			
	Server Connection	Use Pool * Direct			
Access	Server Address	172.45 163.26			
Guided Configuration	Authentication Service Port	1812			
Overview	Secret				
Profiles / Policies	Confirm Secret				
Authentication +					
Single Sign-On	NAS IP Address				
Federation >	NAS IPV6 Address				
Connectivity / VPN	NAS Identifier				
Secure Web Gateway	Timeout	60 seconds			
Access Control Lists	Retries	3			
Webtops	Character Set	UTF-8			
Device Management	Service Type	Default			
Shared Objects	Update Delete				
Network					
System					

- 1. Gehen Sie zu "Main" > "Access" > "Authentication".
- Fügen Sie unter "Configuration" eine "Server Address", den "Authentication Service Port", das "Secret" sowie eine "NAS IP Address" ein.
 <u>Bitte beachten Sie</u>: 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

6	Letty Acoust Delay						
Access	Access Policy: /Common/sparkview_rdp Edit Endings (Indexp End (Adva), Adva)						
Sart)	Salars + - Salars						
Add Net	Nevro III III III III III III III III III I						
An access You can i Please se	a poly institute of a last point, actions, and one or more endings. To invest a new action, this configure an action or ending, data on the last hold below. To delete an action, data on the last poly endines and the last To delete an action, data on the last poly endines. The invest a new action, the last poly endines action, data on the last poly endines and the last to delete an action, data on the last poly endines and the last To delete an action, data on the last poly endines. The invest poly endines action ac						

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:

6								Contraction of the second se
Access Policy: /Common/sparkview_rdp Edit Endings (Endings: Demy (Idrault), Allow)								
	Properties Branch Rules						1	
Start) Start) Start - Sectorated + Sabus + Sabus + Sabus	Name: [Logon Page(1)					c		
fabox +-	Logon Page Agent							
Bad +-es-	Split domain from full Username No 💌							
fallack +-m-	CAPTOHA Configuration	Non	e •					
	Type	Post Variable Na	me	Session Variable Name	Clean Variable	Values	Read Only	
Add New Macro	1 text •	usemame		username	No 🔻		No •	
	2 password •	pessword		password	No. V		No T	
	3 none •	field3	-	Feld3	No T		No *	
We store prior substance of a start point, accord, and one or more enough, to start a new accord, but to the + split a You can not invited with Points Without P. On the new points for these accord Templates and Without a not cive Point	4 none •	field4		Feld4	No •		No •	And where output to and a purpose out, an or proteined active policy time, to employ active policy outputs.
Please set the <u>Online Heats</u> for more Visual Policy Editor basics.	5 none 🔻	field5	=	Fields	No 🔻		No •	and the stand stand stand of the party stands of the stand of the stand of the stand stands.
	Customization						Import	
	Language	en T	_		5	leset all de	tautes	
	1000 A 1000 A 10	Provinsion and the second	-	nourie	14	bella filos		
	Form Header Text	Secure Logon <br< td=""><td>> for PS Netw</td><td>1005</td><td></td><td></td><td></td><td></td></br<>	> for PS Netw	1005				
	Logon Page Input Field	Username						
	Logon Page Input Field	Password						
	Logon Button	Logon	Logon					
	Front Image	Rectars Image I Revert to Default						
	Save Password Checkbox	Save Password	Save Password					
	New Password Prompt	New Password						
	Verify Password Prompt	Verify Password					1	
	Cancel Save						Help	

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.

1 Apoly Access Policy			
Access Policy: /Common/sparkview_rdp Edit Endings (Endings: Deny [dufault], Alow)			7
	Properties Branch Rules		-
Bart	Name: RADIUS Auth		
	RADIUS		
Bad +-m	AAA Server	/Common/DoubleClou •	
falback +-+>	Show Extended Error	Enabled	
	Max Logon Attempts Allowed	3 *	
Add New Marro	Username Source	%(session.logon.last.username)	
	Password Source	%(session.logon.last.password)	
An excess policy results of a set of each actions, and one or more ending. To each are weaking, data on the + each. To early the care per facend with <u>Decirca Minich</u> On the main reception percent <u>Templetes and Wilserds</u> , and click <u>Device Wil</u> Press are the <u>Decirca bine</u> for some Vessal Policy Entities beaux.	Cancel Sere	jed	So the Add Harpe balance had a purpose-balls and <i>af producted</i> account pairs terms, the simplify account pairs (creation, whitry Hamagery Viewed Pairley Editors on the <u>dod's website</u> for more on creating and editing an account pairs.

3.2.3 SSO Credential Mapping

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

1 Apoly Access Policy			Contemport
Access Policy: /Common/sparkview_rdp Edit Endings (Endings: Deny [default], Alow)			
Solitest +	Properties Branch Rules Name: SSO Credential Mapping		-
IP Reputation Bud A state	Variable Assign: SSO Crede	ntial Mapping	
falback	SSO Token Username	mcget (session.logon.lagt.usemame)	
	SSO Token Password	Password from Logon Page *	
Add New Macro		Incet (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			lick 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 ravigation pane, expand Templates and Wizards, and click Device Wiz			alicy 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.			
	Cancel Save		Help