

Integration von Microsoft RD Gateway mit DoubleClue via RADIUS

1. Einführung



Diese Dokumentation ist für Administratoren gedacht, die Fernzugriffe mit Microsoft RD Gateway mit DoubleClue Multi-Faktor-Authentifizierung (MFA) schützen möchten.

Anforderungen:

- Microsoft RD Gateway-Installation
- Installation des DoubleClue Enterprise Management-Systems (DCEM) mit registrierten Benutzern

2. Vorbereitung von DCEM als RADIUS-Server

Sie müssen in DCEM eine "NAS-Client"-Konfiguration hinzufügen.

V DOUBLE CLUE				Enterprise Management
 System Administration Identity Management 	NAS-Clients	n 🗙 Löschen		
OTP Tokens RADIUS NAS-Clients	Name ↓ Keine Einträge vorhanden.	Hinzufügen Name	RD Gateway	×
 RADIUS-Reporting Einstellungen SAML OpenID/OAuth 	Einträge gesamt: 0	IP-Nummer Shared Secret Challenge verwenden Benutzerpasswort ignorieren	172.45.163.88	
UserPortal Version: 22.1		✓ OK 🗶 Ab	brechen	4

- 1. Gehen Sie in DCEM zum Hauptmenüpunkt "RADIUS", Submenü "NAS-Clients", und klicken Sie auf "Hinzufügen".
- 2. Die "IP-Nummer" muss die Quell-IP des Microsoft RD Gateways sein.
- 3. Setzen Sie in der Checkbox "Challenge verwenden" keinen Haken.

4. Klicken Sie auf "OK". Die Konfiguration wird sofort danach wirksam sein.

3. Konfiguration von Microsoft Remote Desktop Gateway

Für eine RDP-Verbindung sendet das RD Gateway eine Zugriffsanfrage an einen RADIUS-Server, welcher in diesem Fall DCEM ist. DoubleClue führt die MFA durch und antwortet mit Accept- oder Reject-Paketen.



Bitte beachten Sie: Benutzerpasswörter werden nicht an den RADIUS-Server gesendet (in diesem Fall DCEM).

- 1. Starten Sie das "RD Gateway Management" und klicken Sie mit der rechten Maustaste auf "Central Network Policy".
- 2. Klicken Sie auf "Configure Central RD-CAP".
- 3. Gehen Sie zum Tab "RD CAP Store".
- 4. Klicken Sie auf den Radio-Button neben "Central server running NPS".
- 5. Fügen Sie die IP-Adresse von DCEM hinzu.
- 6. Falls Sie mehrere DCEM-Knoten verwenden, fügen Sie hier bitte jeden DCEM-Knoten hinzu.
- 7. Klicken Sie auf "OK", um die Konfiguration zu beenden.

RD Gateway Manager	Central Network Policy Servers					
 Policies Control Material Policy 	DC02 Properties				×	
Resource Authorization Policies	Server Farm	Audting	SSL Bridging	Hunging	_	
Monitoring	General	SSL Certificate	Transport Settings	RD CAP Store	2	
	() local server putre					
	Use RD Gat Ocentral server rur Ocentral server rur Ocentral server rur	teway Manager to man teway Manager to man nning NPS and metwork Policy S ath policies for clients	age RD CAPs. erver snap-in to manage P	RD CAPs and to		
	Use RD Gat Ose RD Gat Ose director enforce hea Enter a name or I	ning NPS ning NPS war network Policy S lith policies for clients P address for the serve	age RD CAPs. erver snap-in to manage F r running NPS:	RD CAPs and to		
	Use RD Gat Use RD Gat Order a name or I Order D1 1 1	Ing NPS teway Manager to man ming NPS and methodic Policy S lith policies for clients P address for the serve VS Name 1245.163.88	age RD CAPs. erver snap-in to manage P rrunning NPS:	RD CAPs and to		

3.1 Set the RADIUS Response Timeout

The RADIUS Response time should be increased to at lease 60 or 90 seconds. Within this time the user will have the opportunity to acknowledge the PushApproval.

- 1. In "Network Policy Server", go to "Remote RADIUS Server Groups"
- 2. Select your Server Group and right click on "Properties".
- 3. Select your server and click "edit"
- 4. Go to tab dialog "Load Balancing"
- 5. Set "Number of seconds without response before request is considered dropped to 90 seconds.

Accounting Accounting Accounting	Remote RADIUS Server Groups Image: Remote RADIUS enver groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy. Group Name TS GATEWAY SERVER GROUP TS GATEWAY SERVER GROUP General Group name: TS GATEWAY SERVER GROUP RADIUS Server RADIUS Server Proxy Weight TZASIGUBS 1	Edit RADIUS Server X Address Authentication/Accounting Lead Balancing The priority of ranking indicates the status of a server. A primary server has a priority of 1. Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority. Priority: 1 Weight: 50 Advanced settings Advanced settings Image: Server is identified as unavailable: 12 Number of seconds between request is identified as unavailable: 12 12 12
>	Add Edt. Remove	OK Cancel Apply