

Integration von CISCO Meraki mit DoubleClue via RADIUS

1. Einführung

'cisco' Meraki

Diese Dokumentation ist für Administratoren gedacht, welche die DoubleClue Multi-Faktor-Authentifizierung (MFA) zusammen mit ihrem CISCO Meraki-Produkt verwenden möchten.

2. Vorbereitung von DCEM als RADIUS-Server

Fügen Sie im DoubleClue Enterprise Management-System (DCEM) eine "NAS-Client"-Konfiguration hinzu.

V DOUBLE CLUE				Enterprise Management		
 System Administration Identity Management 	♥ NAS-Clients + Hinzufügen ☞ Ander Name↓	n 🗶 Löschen			Cha	
OTP Tokens		Hinzufügen		×	Chi	
RADIOS NAS-Clients	Keine Einträge vorhanden.	Name	Cisco Meraki		(1 of 1)	
RADIUS-Reporting	Einträge gesamt: 0	IP-Nummer	172.45.160.37			
Einstellungen		Shared Secret	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx			
SAML		Challenge verwenden				
OpenID/OAuth	Benutzerpasswort ignorieren					
UserPortal		✓ OK 🖌 A	Abbrechen			
Version: 2.2.1				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 der CISCO Meraki-Anwendung 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 CISCO Meraki

Client VPN				
Client VPN server 0	Enabled 🗸			
Hostname 0	hostname.123examplehost.com			
Client VPN subnet	172.45.120.0/24]		
DNS nameservers 0	Specify nameservers V			
Custom nameservers	172.45.120.47 172.45.120.48			
WINS O	Specify WINS servers v			
WINS servers	172.45.120.47 172.45.120.48			
Secret	2	Hide	ernt	
	PADUS			
Authentication	100003			
Authentication				
Authentication RADIUS servers	Host	Port	Secret	Act

Hier können Sie eine typische RADIUS-Konfiguration von CISCO Meraki sehen.

Bitte überprüfen Sie, dass der Port mit demjenigen, welchen Sie in DCEM konfiguriert haben und den Sie unter dem Hauptmenüpunkt "System", Untermenü "Cluster-Konfigurationen", Eintrag "RADIUS Authentication" einsehen und konfigurieren können, übereinstimmt.

4. Timeout-Konfiguration

DoubleClue verwendet mobile Endgeräte für die MFA. Während der Authentifizierungsphase benötigt der Benutzer möglicherweise einige Zeit, um sein Mobilgerät einzuschalten, die DoubleClue-App zu starten und die Meldungen zu bestätigen.

4.1 CISCO Meraki-Timeout

Der Standard-Timeout für CISCO Meraki ist 5 Sekunden für 3 Versuche. Dies bedeutet, dass Benutzer insgesamt nur 15 Sekunden haben, was möglicherweise zu kurz ist. Wir empfehlen, die Timeout-Dauer zu verlängern.

Sie können die Timeout-Dauer in der Konfigurations-GUI von CISCO Meraki nicht ändern. Bitte kontaktieren Sie für Änderungen den Meraki-Support unter <u>https://meraki.cisco.com/support/</u>

Wir empfehlen 60 Sekunden x 3 Versuche.

4.2 Windows 10 Timeout

Der Standard-Timeout des Windows 10 VPN Client beträgt 30 Sekunden, was möglicherweise zu kurz für den Benutzer ist, um sein Mobilgerät einzuschalten und die Authentifizierungsmeldung zu bestätigen.

Um die Dauer bis zum Timeout zu verlängern, müssen Sie in der Windows-Registrierung die folgenden Einstellungen ändern.

Wir empfehlen, die Dauer ebenfalls auf 3 Minuten zu erhöhen. Der Windows 10 Client wiederholt mit einer Rate von 3 Sekunden, daher wird die Anzahl der Wiederholungen auf 60 gesetzt:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\MaxConfigure = 60 (decimal)

und

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\MaxFailure = 60 (decimal)

> KasAuto	^ Name	Тур	Daten
> Rasl2tp ▼ RasMan	(Standard)	REG_SZ	(Wert nicht festgelegt)
IKEv2	DIIName	REG_SZ	rasppp.dll
 Parameters PPP ControlProtocols EAP 	100 MaxConfigure	REG_DWORD	0x0000020 (32)
	👪 MaxFailure	REG_DWORD	0x00000020 (32)
	500 MaxReject	REG_DWORD	0x00000005 (5)
	88 MaxTerminate	REG_DWORD	0x0000002 (2)
Security	👪 Multilink	REG_DWORD	0x0000000 (0)
ThirdParty	🕮 NegotiateTime	REG_DWORD	0x00000096 (150)
> RasPppoe	🕮 Restart Timer	REG_DWORD	0x0000003 (3)
> RasSstp			