****

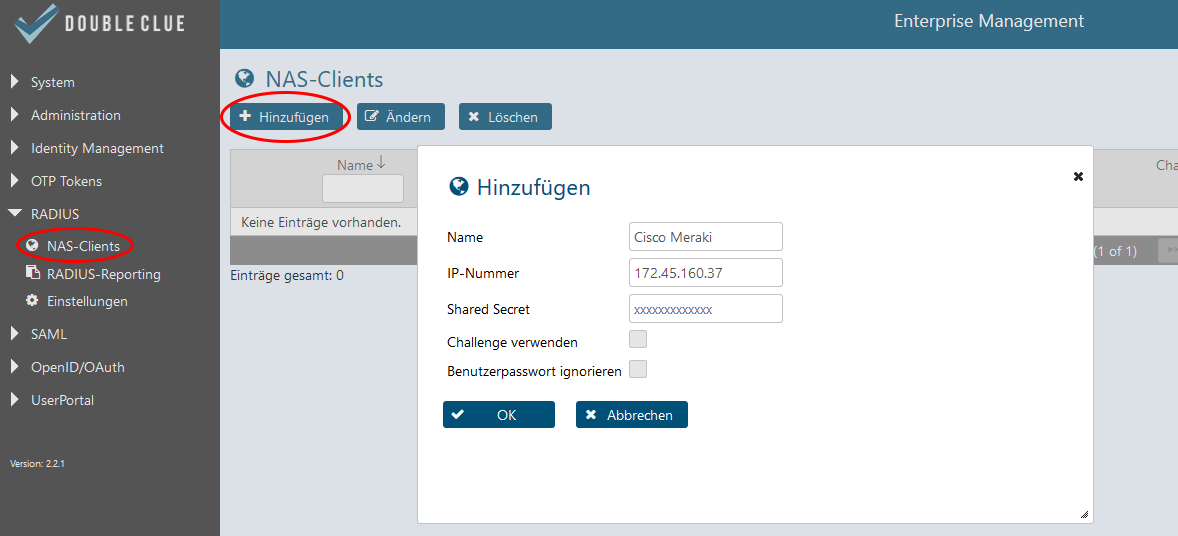
Integration von CISCO Meraki mit DoubleClue via RADIUS

# C:\Users\maike.behnsen\Documents\DoubleClue\Logos\Externe Logos\Logo_Cisco_Meraki.pngEinführung

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

# Vorbereitung von DCEM als RADIUS-Server

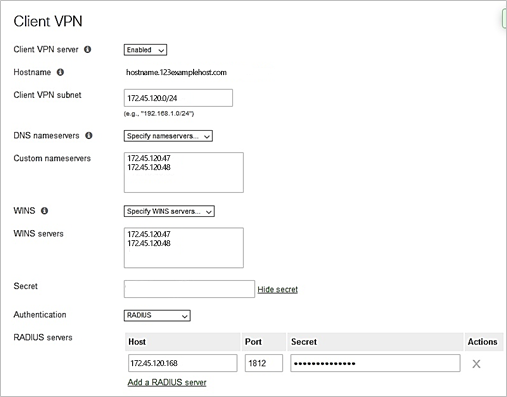
Fügen Sie im DoubleClue Enterprise Management-System (DCEM) eine „NAS-Client“-Konfiguration hinzu.



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.

# Konfiguration von CISCO Meraki

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.

# 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.

## 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 <https://meraki.cisco.com/support/>

Wir empfehlen 60 Sekunden x 3 Versuche.

## 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)*

