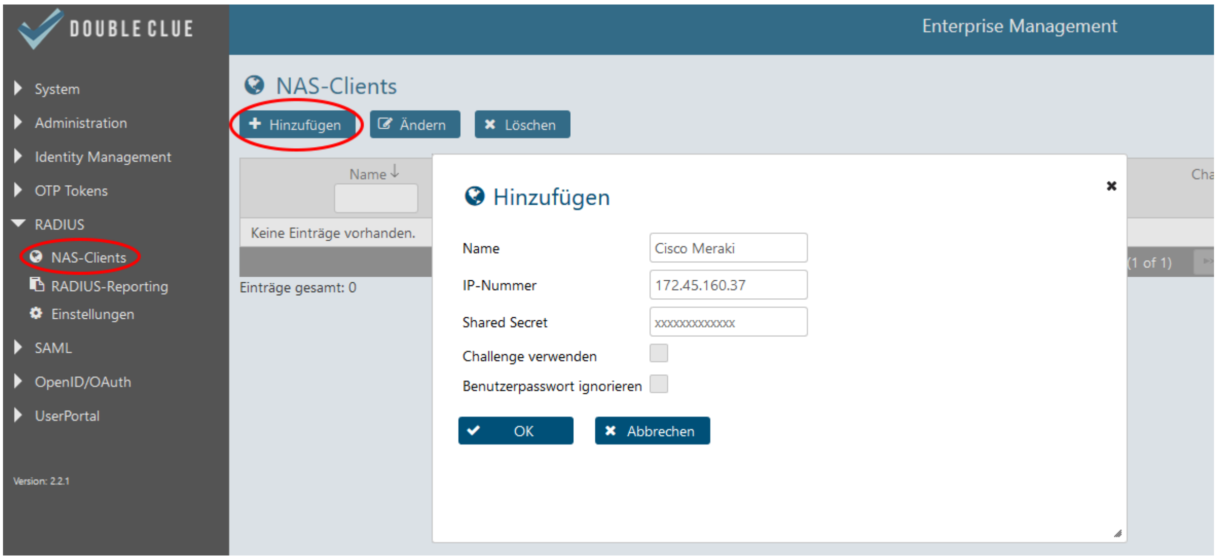
Integration of CISCO Meraki with DoubleClue using RADIUS

1. Introduction

This guide is intended to help administrators to use DoubleClue Multi-Factor Authentication (MFA) together with their CISCO Meraki product.

2. Preparing DCEM as a RADIUS Server

You need to add a "NAS Client" configuration in DoubleClue Enterprise Management (DCEM).



Hinzufügen

Name: Cisco Meraki

IP-Nummer: 172.45.160.37

Shared Secret: xxxxxxxxxxxxx

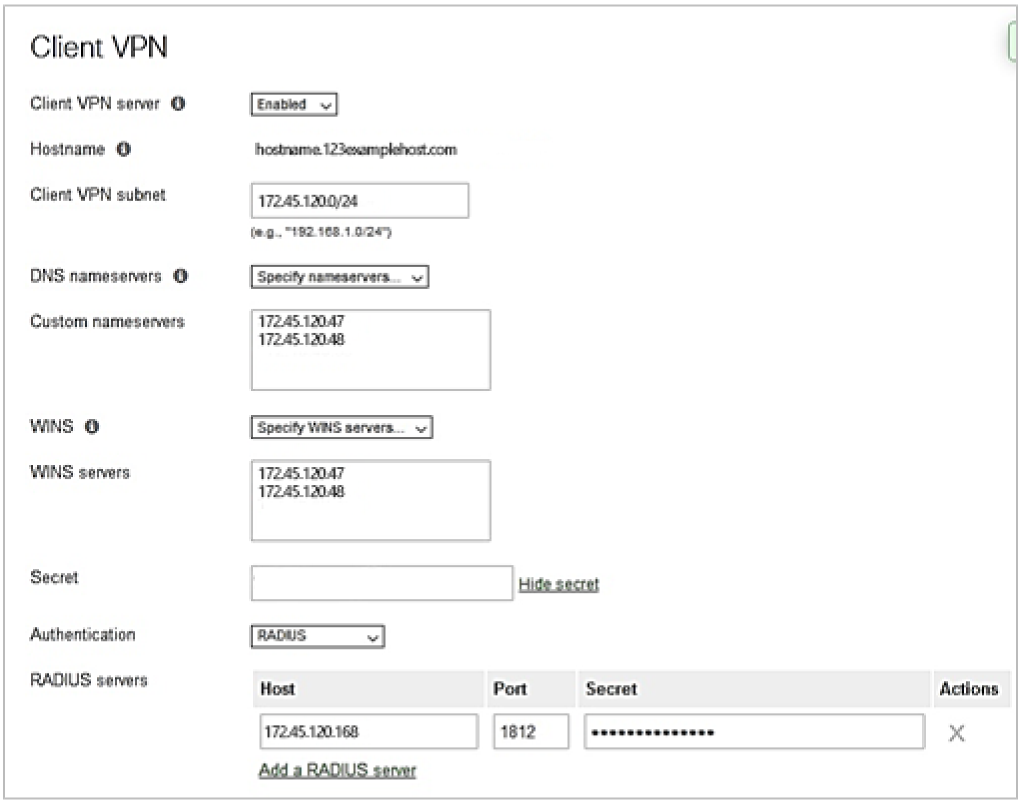
Challenge verwenden ☐

Benutzerpasswort ignorieren ☐

1. In DCEM, go to main menu item "RADIUS", sub menu "NAS Clients" and click on "Add".
2. The "IP Number" must be the source IP of the CISCO Meraki appliance.
3. Do not enable the checkbox "Use Challenge".
4. Click on "OK". The configuration will be active immediately after that.

3. CISCO Meraki Configuration

Here you can see a typical CISCO Meraki RADIUS configuration.



Client VPN

Client VPN server: Enabled

Hostname: hostname.123examplehost.com

Client VPN subnet: 172.45.120.0/24
(e.g., "192.168.1.0/24")

DNS nameservers: Specify nameservers...

Custom nameservers: 172.45.120.47
172.45.120.48

WINS: Specify WINS servers...

WINS servers: 172.45.120.47
172.45.120.48

Secret: Hide secret

Authentication: RADIUS

RADIUS servers

Host	Port	Secret	Actions
172.45.120.168	1812	•••••••••••••••	×

Add a RADIUS server

Please verify that the port matches with the port configured in DCEM, which you can view under main menu item “RADIUS”, sub menu “Preferences”.

4. Timeout Configuration

DoubleClue does MFA using mobile devices. During the authentication phase, the user may require some time to switch on their mobiles, start the DoubleClue App and confirm the messages.

4.1 CISCO Meraki Timeout

The default timeout for CISCO Meraki is 5 seconds for 3 attempts. In total this means that users have only 15 seconds, which may be too short. We recommend extending this timeout period.

You cannot change the timeout period in the CISCO Meraki configuration GUI. Please contact CISCO Meraki Support at https://meraki.cisco.com/support/ to change it.

We recommend 60 seconds x 3 attempts.

4.2 Windows 10 Timeout

The default Windows 10 VPN Client timeout is 30 seconds, which may be too short for users to switch on their mobiles and confirm the authentication message.

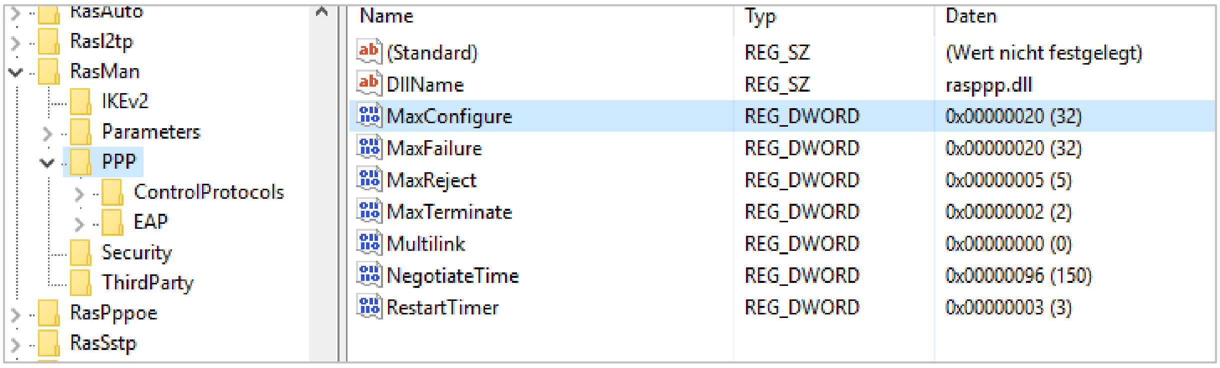
In order to increase the timeout period, you have to change the following windows registration settings.

We recommend extending this period to 3 minutes, too. The Windows 10 Client repeats at a rate of 3 seconds, so we will set the number of repetitions to 60:

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

and

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



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
DllName	REG_SZ	rasppp.dll
MaxConfigure	REG_DWORD	0x00000020 (32)
MaxFailure	REG_DWORD	0x00000020 (32)
MaxReject	REG_DWORD	0x00000005 (5)
MaxTerminate	REG_DWORD	0x00000002 (2)
Multilink	REG_DWORD	0x00000000 (0)
NegotiateTime	REG_DWORD	0x00000096 (150)
RestartTimer	REG_DWORD	0x00000003 (3)