Integration of Microsoft RD Gateway with DoubleClue using RADIUS

1. Introduction

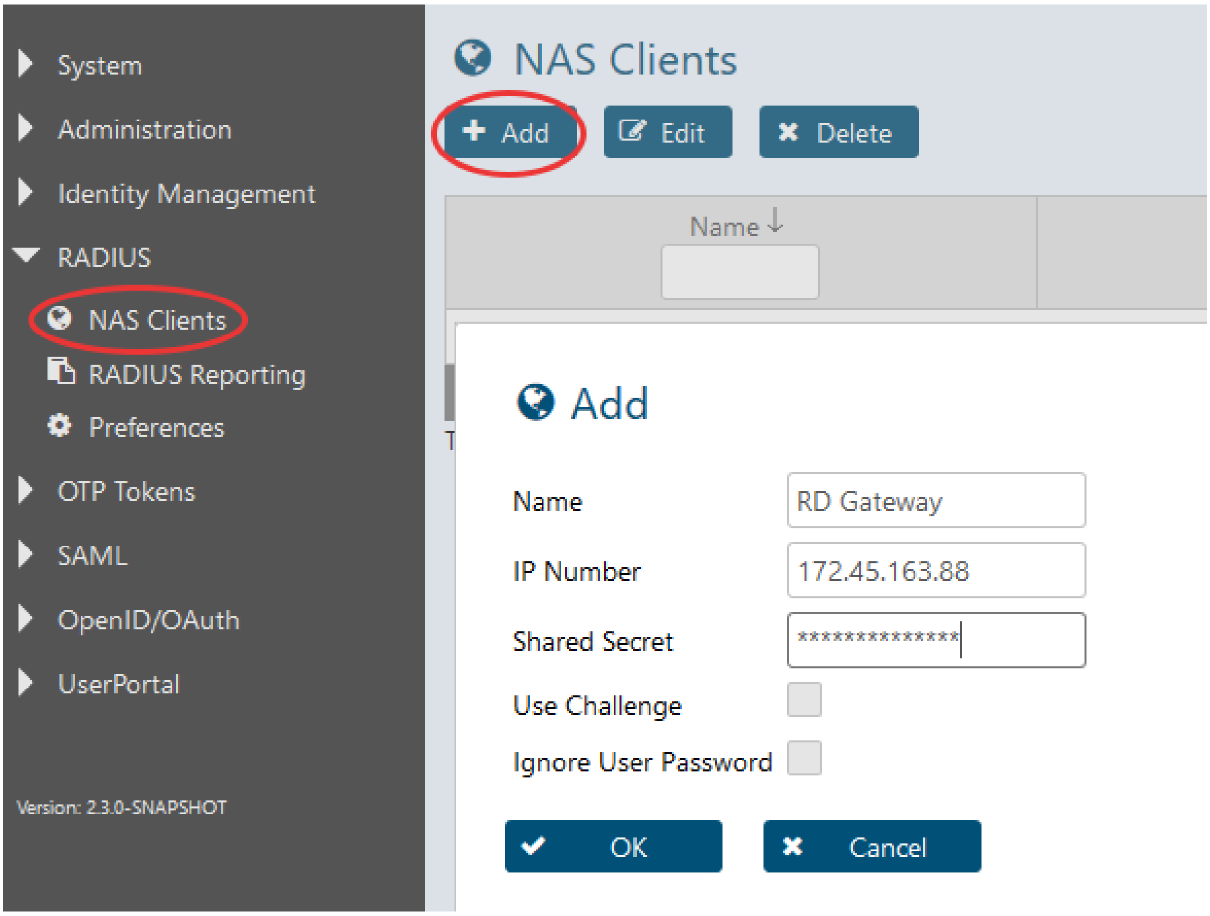
This guide is intended for administrators who would like to protect their Microsoft RD Gateway remote access using DoubleClue Multi-Factor Authentication (MFA).

Requirements:

- Installation of Microsoft RD Gateway.
- DoubleClue Enterprise Management (DCEM) installation with readily registered users.

2. Preparing DCEM as a RADIUS Server

You need to add a “NAS Client” configuration in DCEM.



Name	RD Gateway
IP Number	172.45.163.88
Shared Secret	**************
Use Challenge	□
Ignore User Password	□

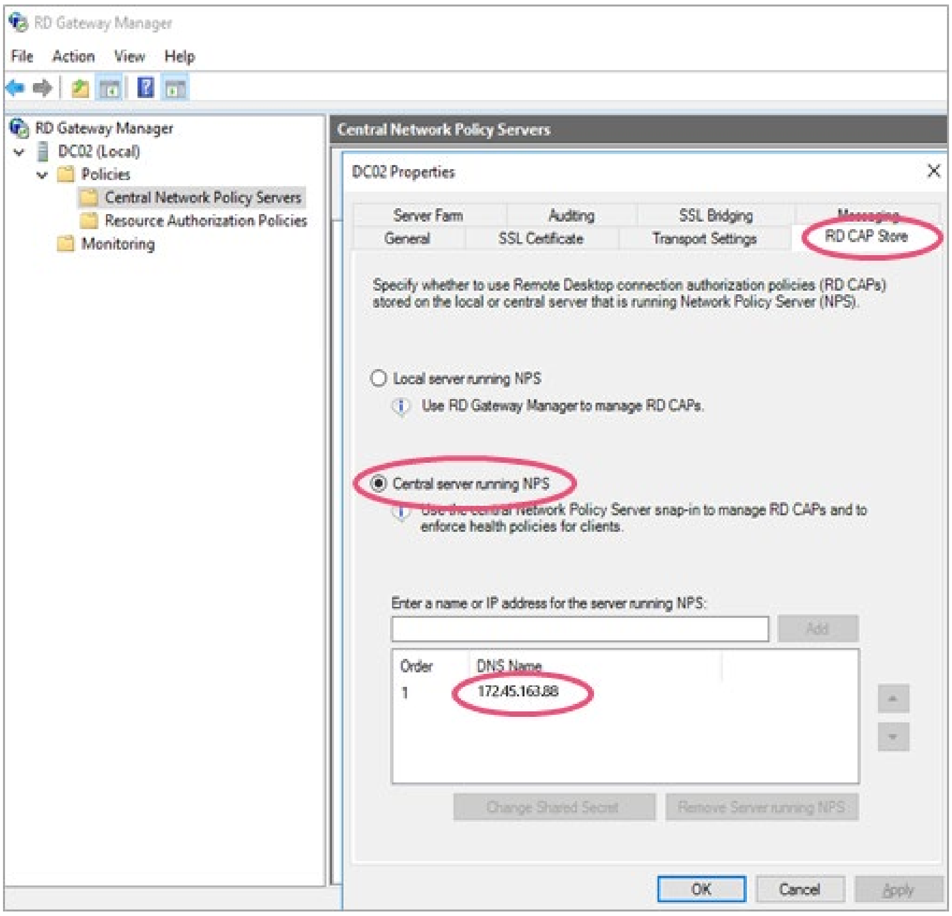
1. In DCEM, go to main menu item “RADIUS”, sub menu “NAS Clients” and click on “Add”.
2. The “IP Number” must be the source IP of the Microsoft RD Gateway.
3. Do not enable the checkbox “Use Challenge”.
4. Click on “OK”. The configuration will be active immediately after that.

3. Microsoft RD Gateway Configuration

For an RDP connection, the RD Gateway will send an Access request to a RADIUS Server, which is DCEM in this case. DoubleClue will perform the MFA and response with Accept or Reject packets.

⚠ Please note: User passwords are not sent to the RADIUS Server (in this case DCEM).

1. Start “RD Gateway Management” and right click on “Central Network Policy”
2. Click on “Configure Central RD-CAP”.
3. Go to the tab “RD CAP Store”
4. Check the radio button next to “Central server running NPS”.
5. Add the IP address of DCEM.
6. If you are using several DCEM nodes, please add each DCEM node here.
7. Click on “OK” to finish the configuration.



Specify whether to use Remote Desktop connection authorization policies (RD CAPs) stored on the local or central server that is running Network Policy Server (NPS).

○ Local server running NPS

Use RD Gateway Manager to manage RD CAPs.

● Central server running NPS

Use the central Network Policy Server snap-in to manage RD CAPs and to enforce health policies for clients.

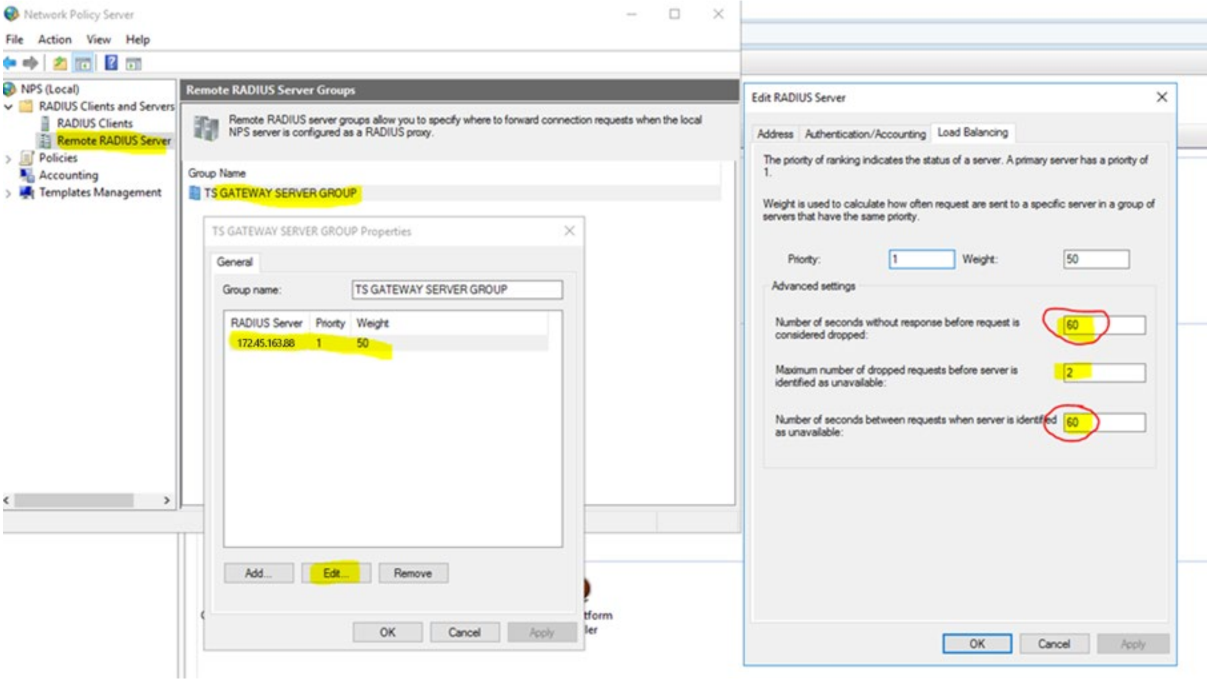
Enter a name or IP address for the server running NPS:

Order	DNS Name
1	172.45.163.88

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.



Remote RADIUS server 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

Group name: TS GATEWAY SERVER GROUP

RADIUS Server	Priority	Weight
172.45.163.88	1	50

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

Number of seconds without response before request is considered dropped: 60

Maximum number of dropped requests before server is identified as unavailable: 2

Number of seconds between requests when server is identified as unavailable: 60