

Integration of Microsoft RD Gateway with DoubleClue using RADIUS

1. Introduction



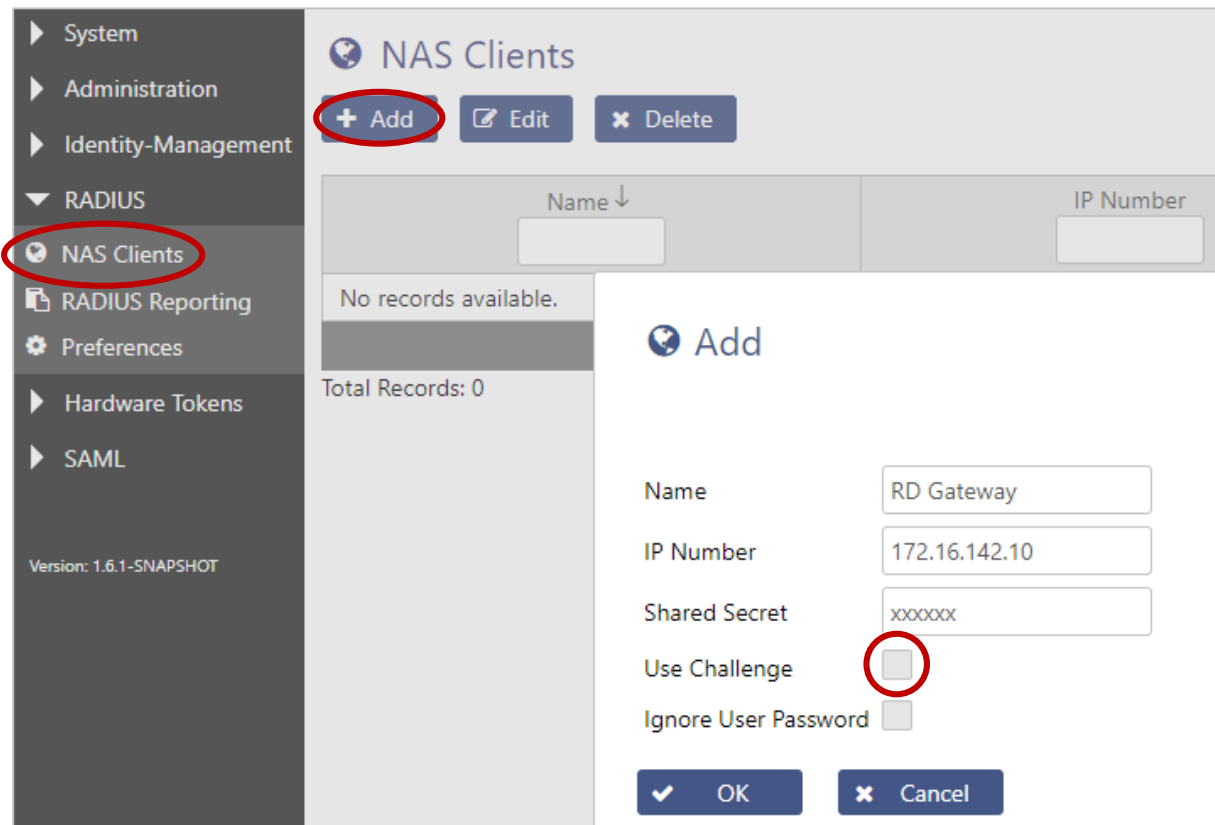
This guide is intended for administrators who would like to protect their Microsoft RD Gateway remote access using DoubleClue Multi-Factor Authentication (MFA).

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.



The screenshot displays the DCEM interface for managing RADIUS clients. The left sidebar shows the navigation menu with 'NAS Clients' selected. The main area shows the 'NAS Clients' configuration page with an 'Add' button circled in red. The 'Add' dialog box is open, showing the following fields:


- Name: RD Gateway
- IP Number: 172.16.142.10
- Shared Secret: xxxxxx
- Use Challenge: (circled in red)
- Ignore User Password:

The dialog box also includes 'OK' and 'Cancel' buttons.

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.

