NetMotion Integration with GreenRADIUS - Quick Start Guide

December 11, 2017

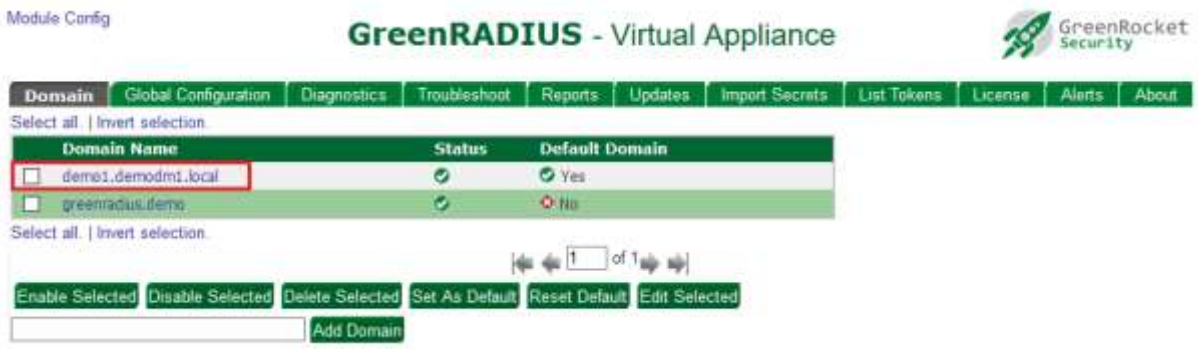
Contents

1 GreenRADIUS Setup

Before starting, ensure GreenRADIUS is configured correctly to communicate with the local Active Directory or LDAP domain, as well as with the validation service (either local validation or the YubiCloud). Full instructions on setting up GreenRADIUS can be found in the GreenRADIUS Configuration Guide, available on the Green Rocket Security Website here: http://www.greenrocketsecurity.com/resources/library/.

1.1 General Configuration

1. Open the GreenRADIUS Web admin interface and navigate to the Domain tab.
2. Create a new domain for importing users from Active Directory. Use the same domain name as that of the name of domain in Active Directory. See the image given below.



1.2 Domain Configuration

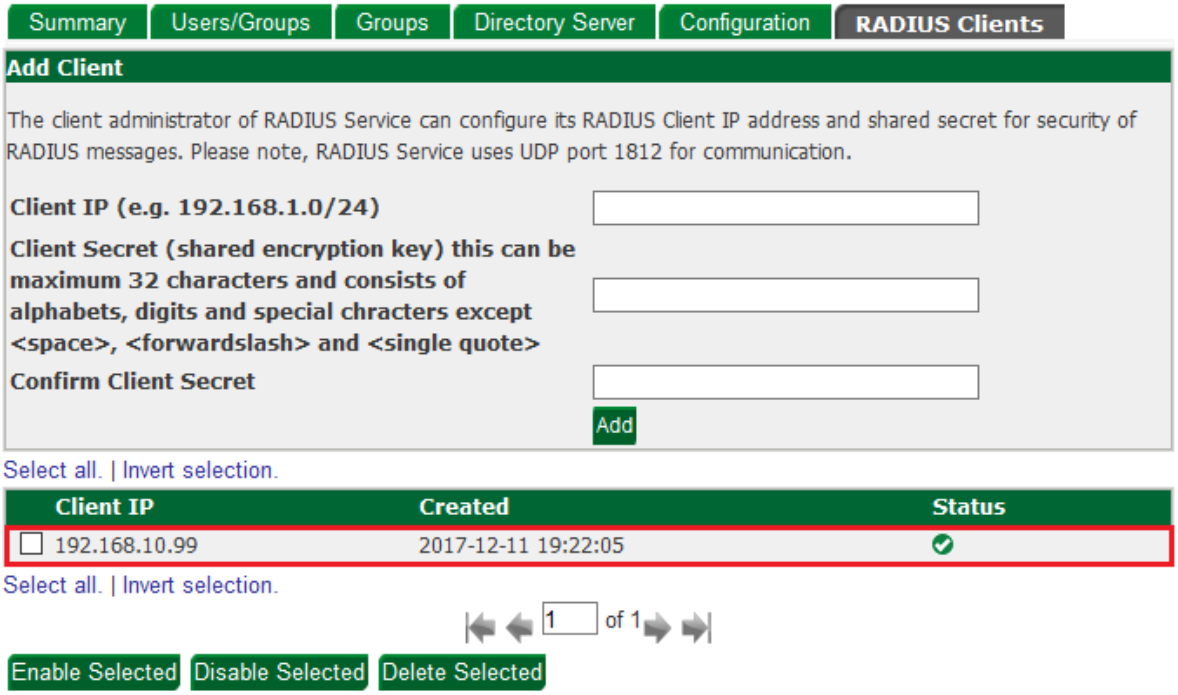
1. After creating the domain, import users from Active Directory. Assign a token to one or more users. These token assigned-users will be used for two-factor authentication for NetMotion.

2. Click on the “RADIUS Clients” tab, enter the following details about the NetMotion Mobility Server installation:

    a. Client IP – enter in the IP address of the NetMotion Mobility Server. If you enter an IP address that ends with 0/24, (such as 192.168.1.0/24), GreenRADIUS will accept a request from client across the entire subnet on the selected port.

    b. Client Secret / Confirm Client Secret – This is a symmetric shared secret between the GreenRADIUS server and the NetMotion Mobility server. Please follow best practice with secure password policies when creating this shared secret. GreenRADIUS can hold a secret of up to 50 characters.

3. Click the “Add” button below the fields to add the NetMotion Mobility Server to GreenRADIUS. Once done, the details entered will appear below.

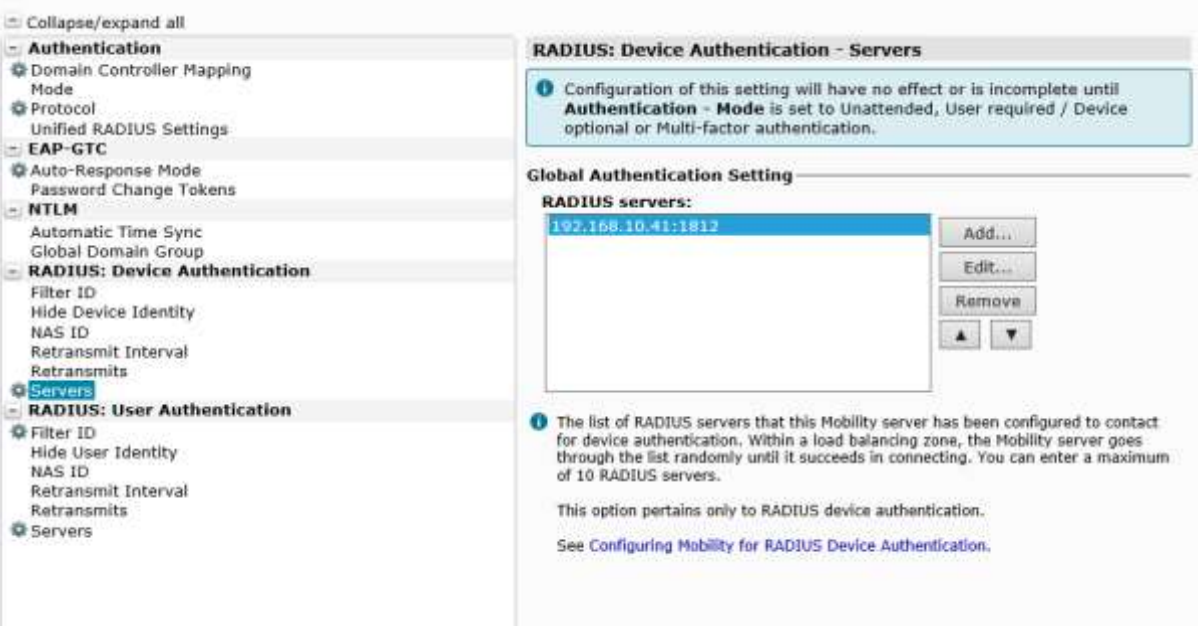


2 NetMotion Mobility Server Configuration

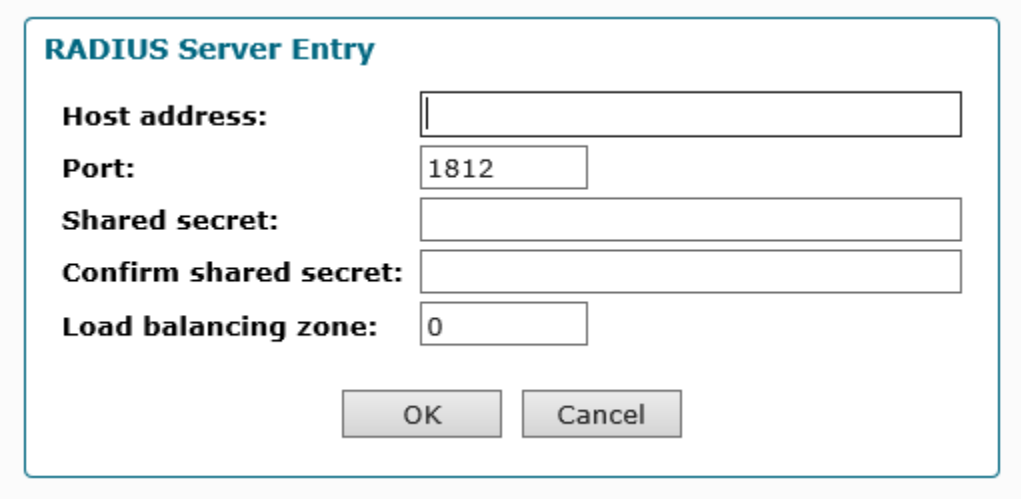
Before starting, ensure NetMotion Mobility is configured correctly using user credentials stored in an Active Directory / LDAP server. Full instructions on setting up NetMotion Mobility Server can be found at the following link:
https://help.netmotionsoftware.com/support/docs/MobilityXG/1100/help/mobilityhelp.htm

1. Log in to the NetMotion Mobility console (web interface).
2. In the Main Menu, click on the "Configure" tab and select "**Authentication Settings**".
3. Locate "Authentication Settings", and then select the "Protocol" option. In the Authentication – Protocol page, set the Protocol to RADIUS – EAP (PEAP and EAP-TLS), then click Apply.

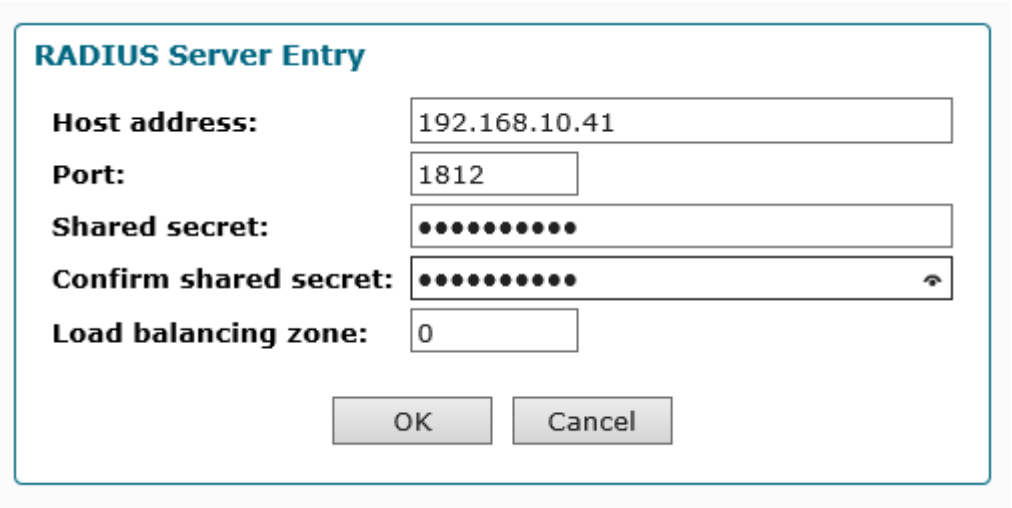
4. In the Authentication - RADIUS: Device Authentication - Servers page, click the Add button. This will open the RADIUS Server Entry Page.



5. In the RADIUS Server Entry Page, locate the field labelled “Host address” and enter the IP address of GreenRADIUS.

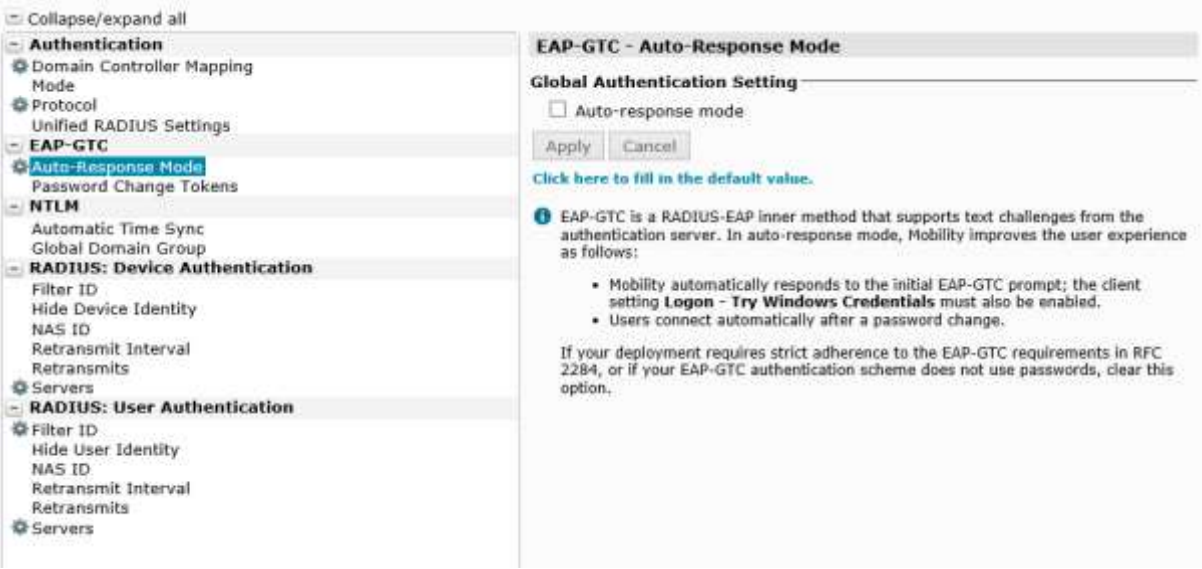


6. Locate the “Port” field, and verify it is automatically populated with the default RADIUS port value 1812.
7. Locate the “Shared secret” field and enter in the same Client Secret used in GreenRADIUS. The Shared Secret must match the Client Secret exactly.
8. Confirm the Shared Secret by typing it in again in the “Confirm shared secret” field.
9. Click the “OK” button. The Newly created RADIUS server profile should be displayed in the RADIUS Server menu.

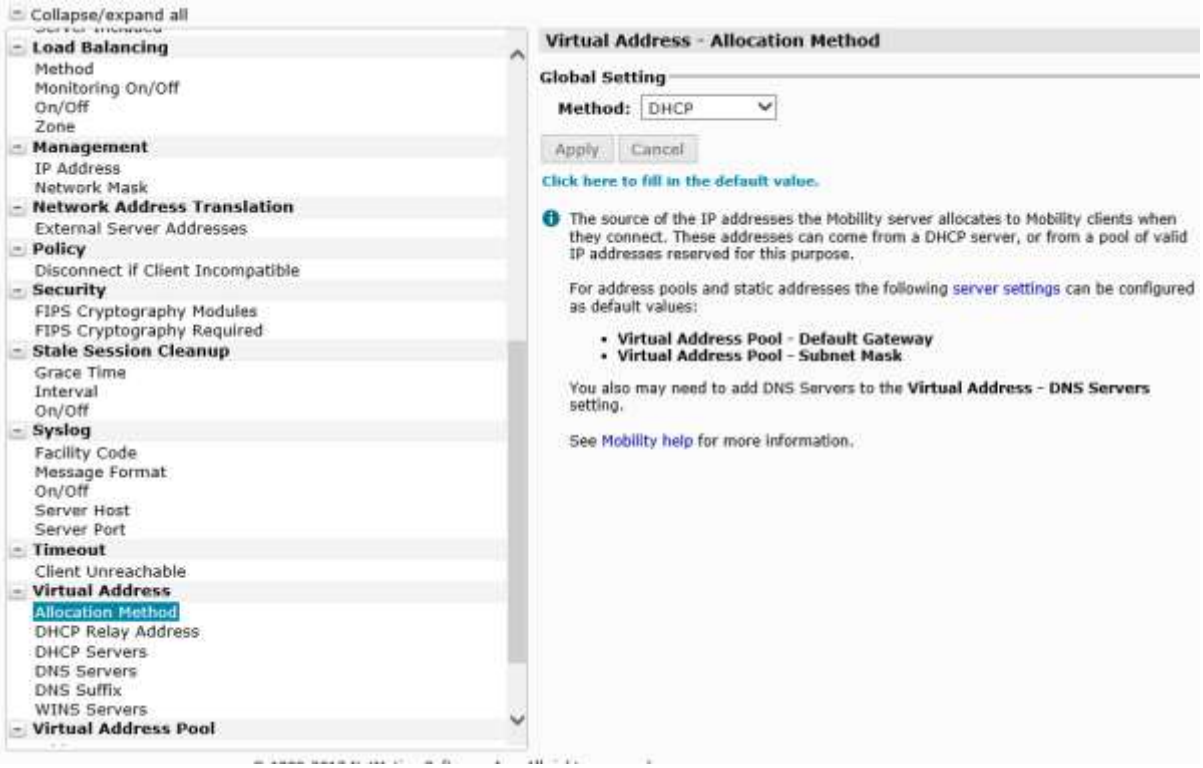


10. The new RADIUS Server entry should now be listed in the RADIUS servers section.
11. Repeat the steps 5-11 for **RADIUS: User Authentication** > Servers.

12. Locate and click “Authentication >> **EAP-GTC** => Auto-Response Model”. Uncheck the checkbox “Auto-response mode” and click on “Apply”.

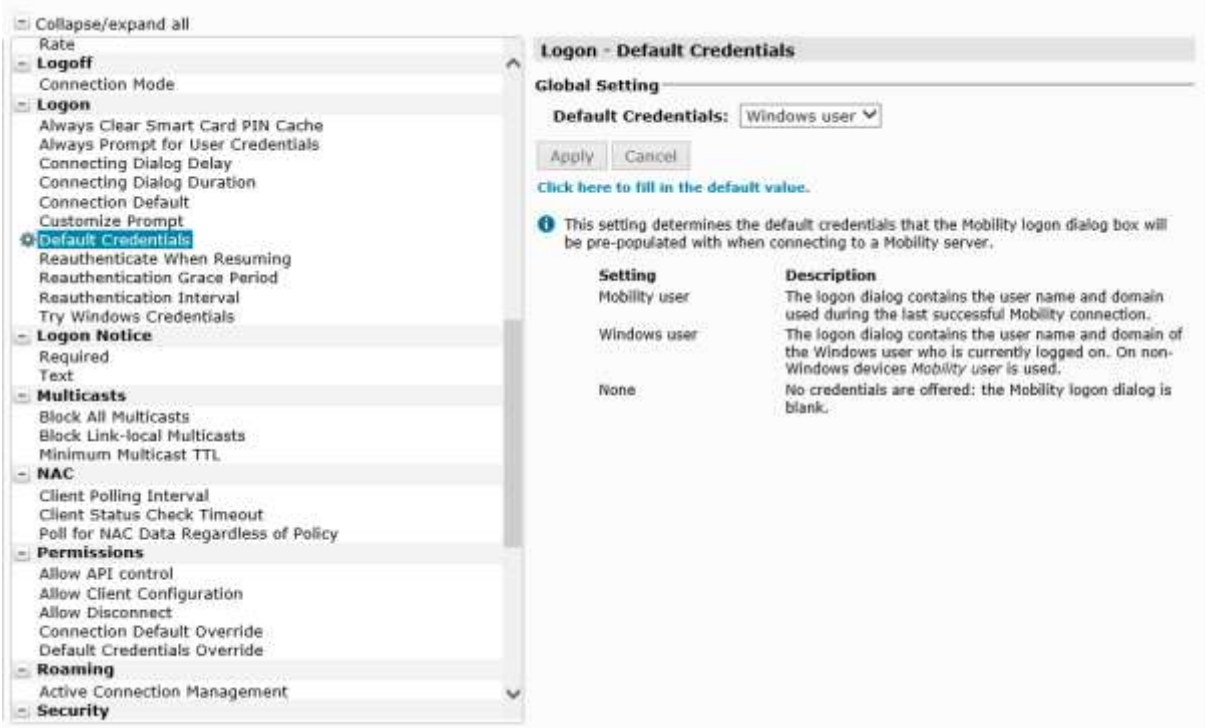


13. Locate the option “Configure >> Server Settings >> Virtual Address” and select “Allocation Method”. Then, choose the “DHCP” method from the drop down menu and click on “Apply”.



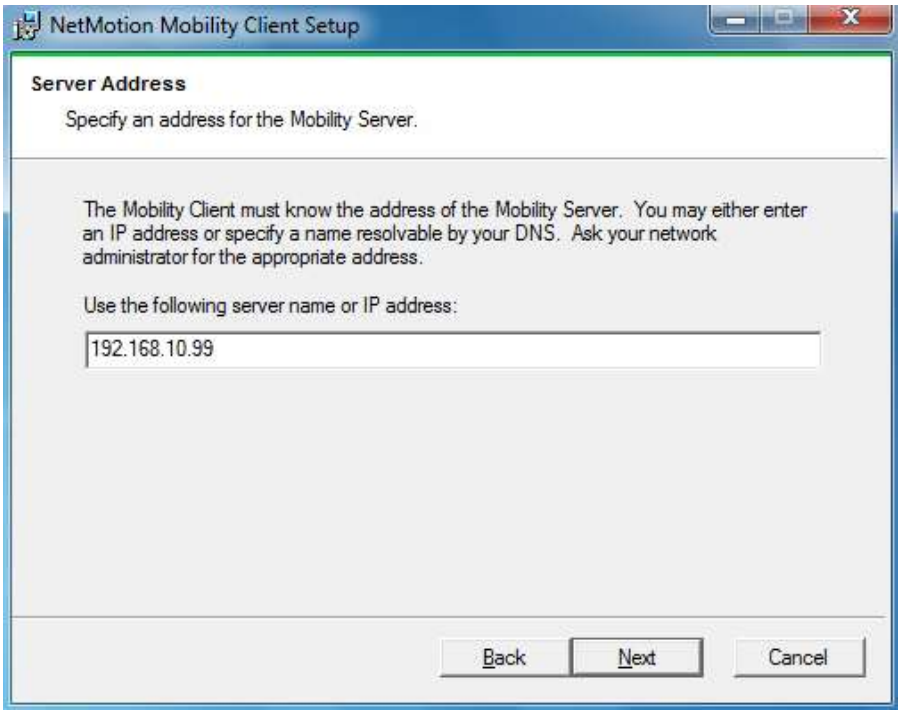
14. In the Main Menu, click on the “Configure” tab, and select “**Client Settings**”.

15. Locate and click “**Logon** >> Default Credentials” and select the “Windows user” option. Then click on “Apply”.



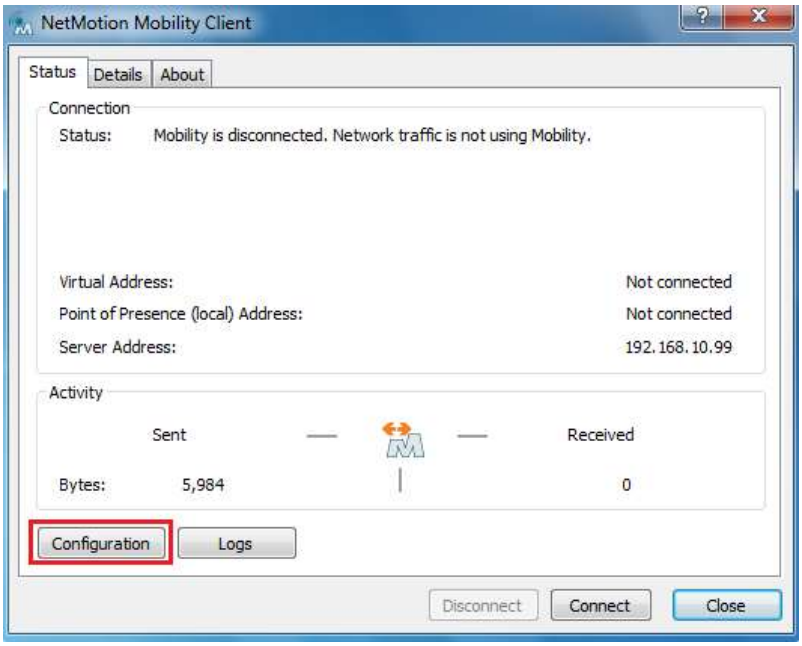
3 NetMotion Mobility Client Configuration

1) Configure one or more Windows clients, and add them to your Active Directory Domain Services.
2) Access the Windows client using Active Directory's administrator credentials for installing the Netmotion Mobility Client.
3) Then, install the NetMotion Mobility client. Setup is like any other software executable install package. But carefully enter the NetMotion server IP address as shown in the image below:

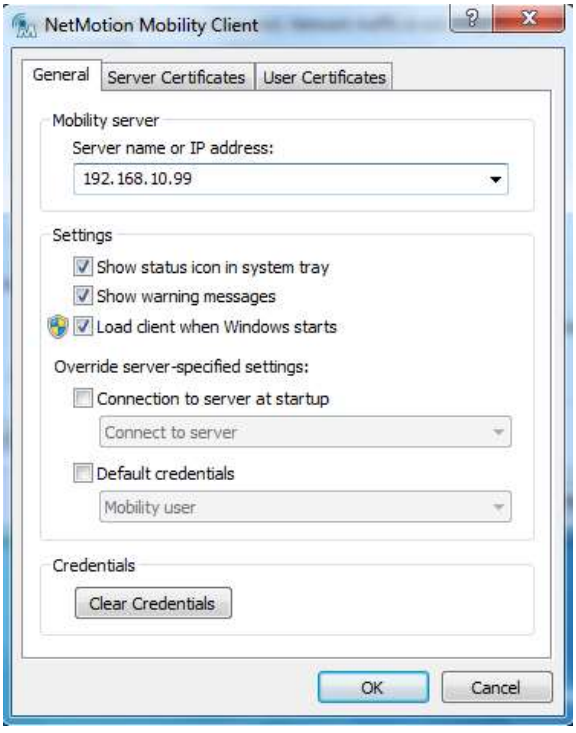


4) Setup will ask for restarting the computer. Otherwise, manually restart the computer.
   Note: After restarting, log in to the client as administrator. The following screen may appear, because the NetMotion Mobility Client is not yet configured. Simply press "Skip".

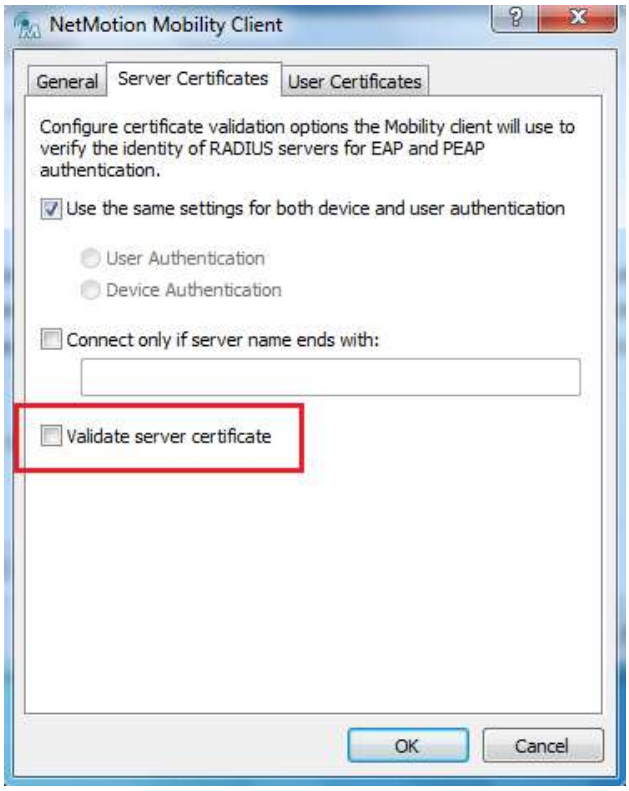
5) Now, configure the Windows client. Search for the "Mobility Client" application and open it. The following window will open. Then click on the "Configuration" option.



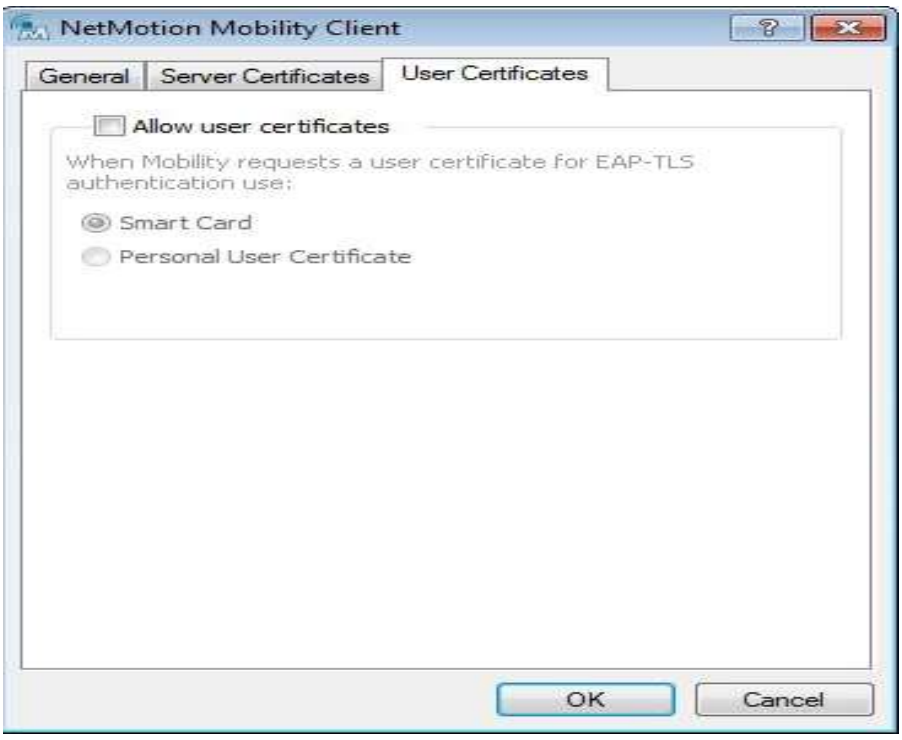
6) After clicking “Configuration”, the following window will open. Select the “Server Certificates” tab.



7) In the “Server Certificates” tab, uncheck the “Validate Server Certificate” checkbox.

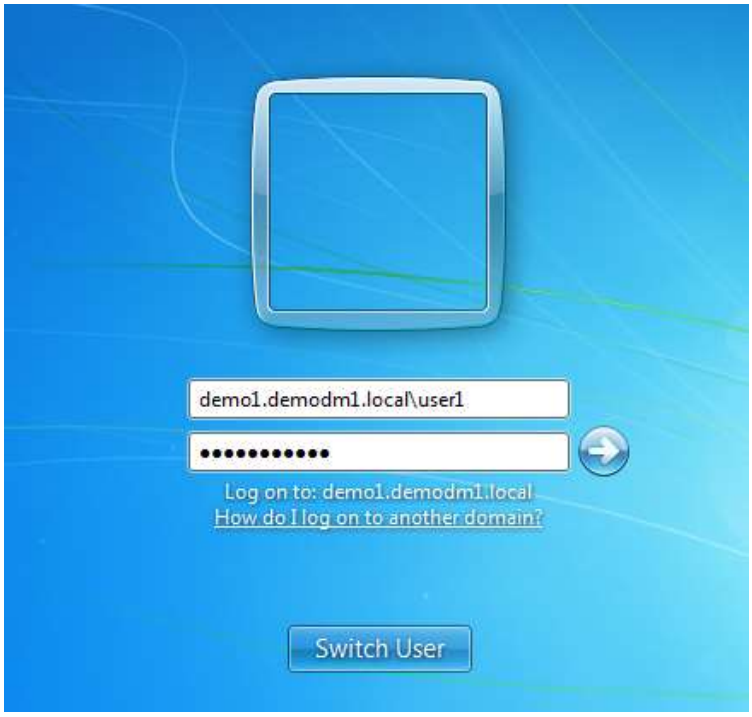


8) Select the “User Certificates” tab, and uncheck “Allow User Certificates”. Then press “OK”.

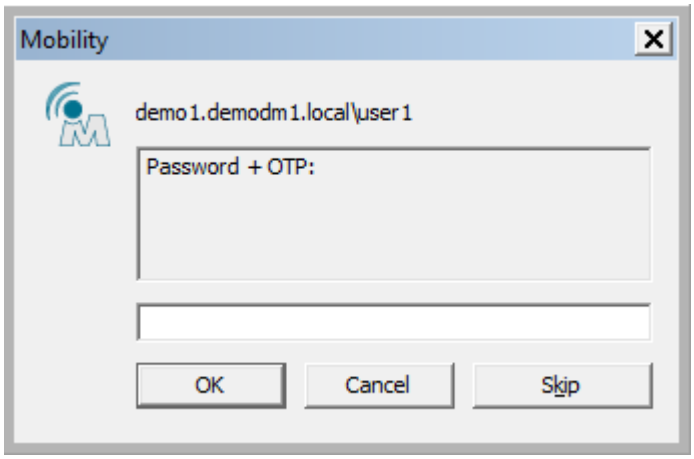


9) We have successfully configured the “Netmotion Mobility Client”. Now, restart the system.

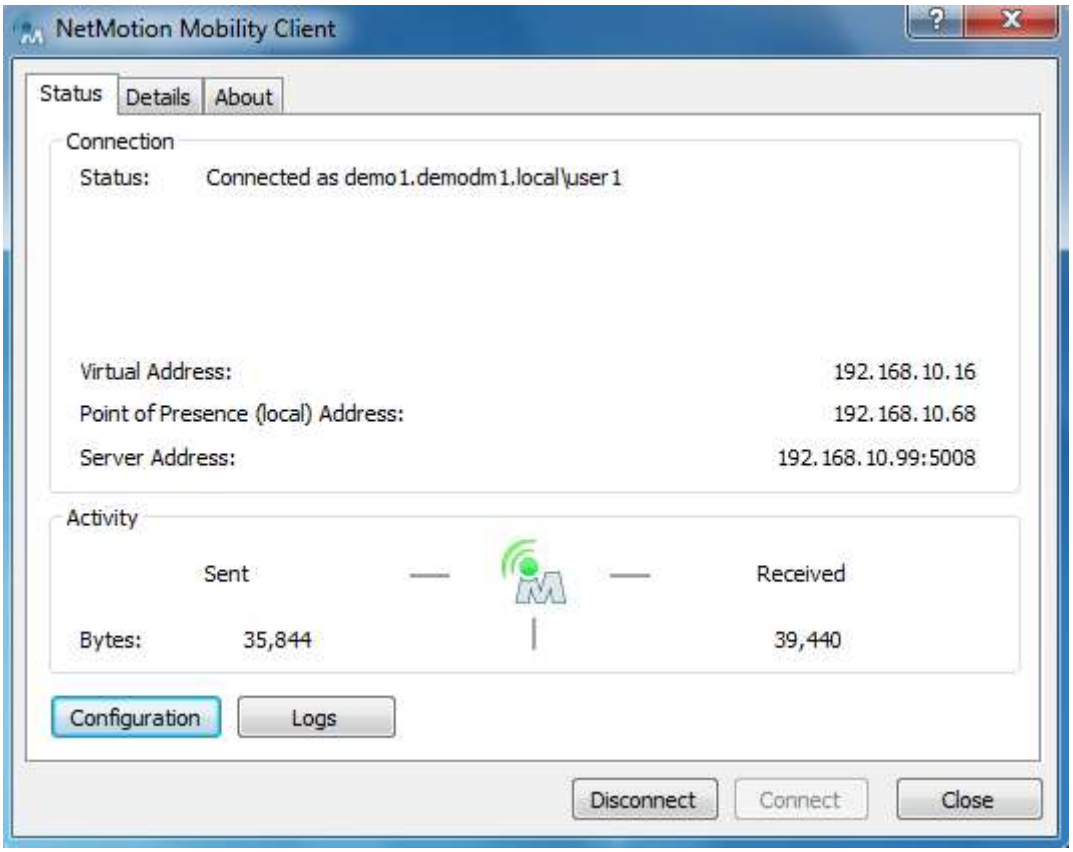
10) Important -- After restarting the computer, log in using the user to which a token is assigned. For example, in the image shown below, “user1” of the “demo1.demodm1.local” domain is used for logon.



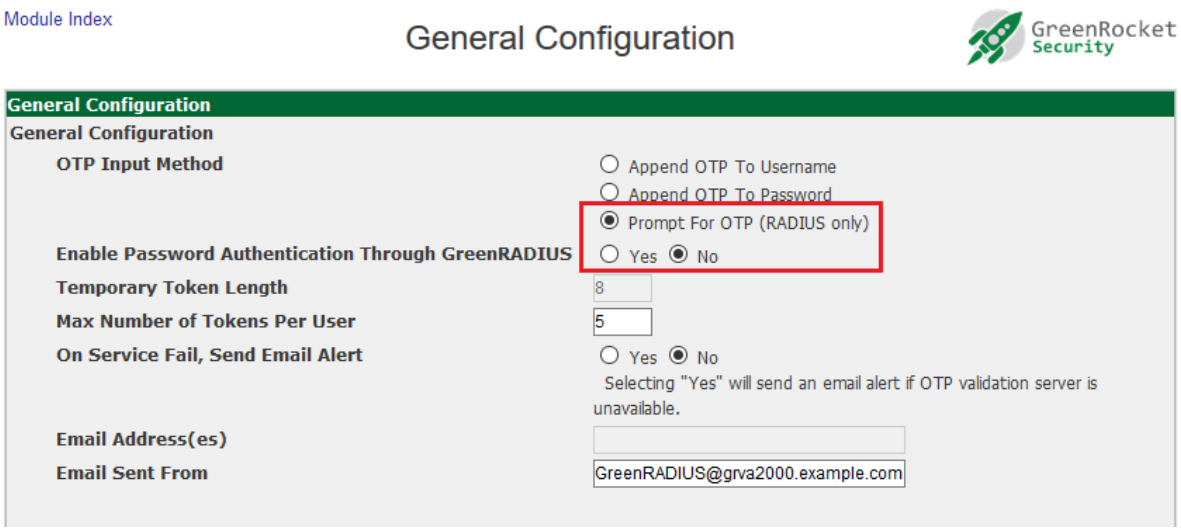
11) After logging into the PC, the Mobility window will appear. Enter the user’s password and append the token’s OTP, then press “OK”.



12) If the password and OTP are correct, then NetMotion will connect to the server, and the network will become active. NetMotion will also show the status as “Connected”.



13) It is also possible to avoid submitting the user's password twice (at Windows Logon and then in the Mobility Client) by changing the GreenRADIUS authentication to OTP only. Navigate to the Global Configuration tab --> General. Under OTP Input Method, select **Prompt for OTP (RADIUS only)** and select **No** under "Enable Password Authentication Through GreenRADIUS". Save the settings. (Note: This configuration should only be used if GreenRADIUS is only used for NetMotion.)



14) Now, only an OTP may be submitted directly without a password at the Mobility login.