Cisco Remote Access with GreenRADIUS 2FA - Integration Guide

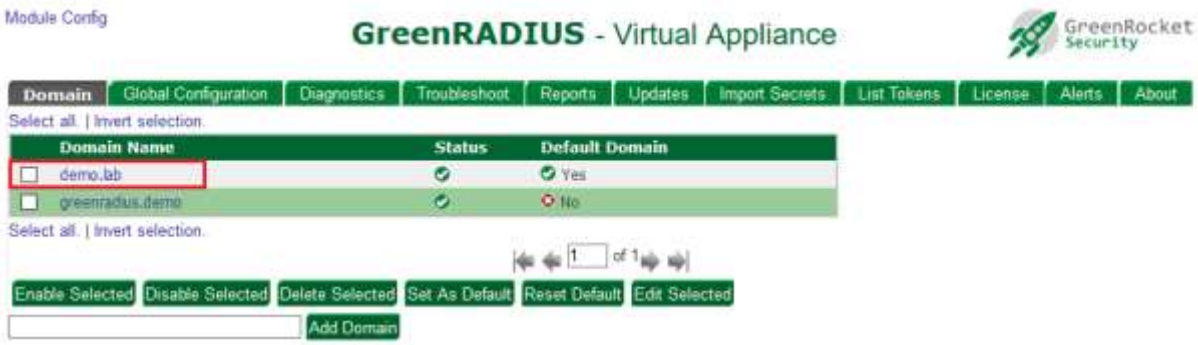
January 23, 2018

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 our Document Library -- 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 the domain in Active Directory. See the image below.



1.2 Domain Configuration

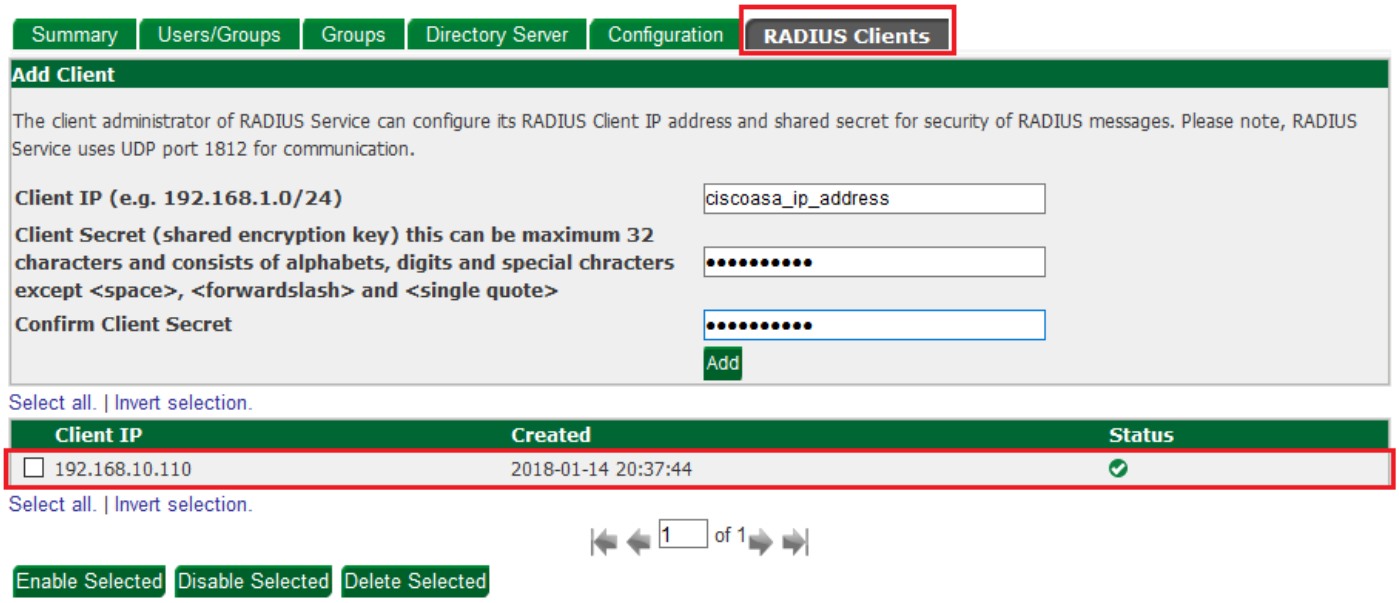
1. After creating the domain, import users from Active Directory. Assign a token to one or more users. These tokens will be used for two-factor authentication.

2. Click on the “RADIUS Clients” tab, and enter the following details about your Cisco ASA:

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

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

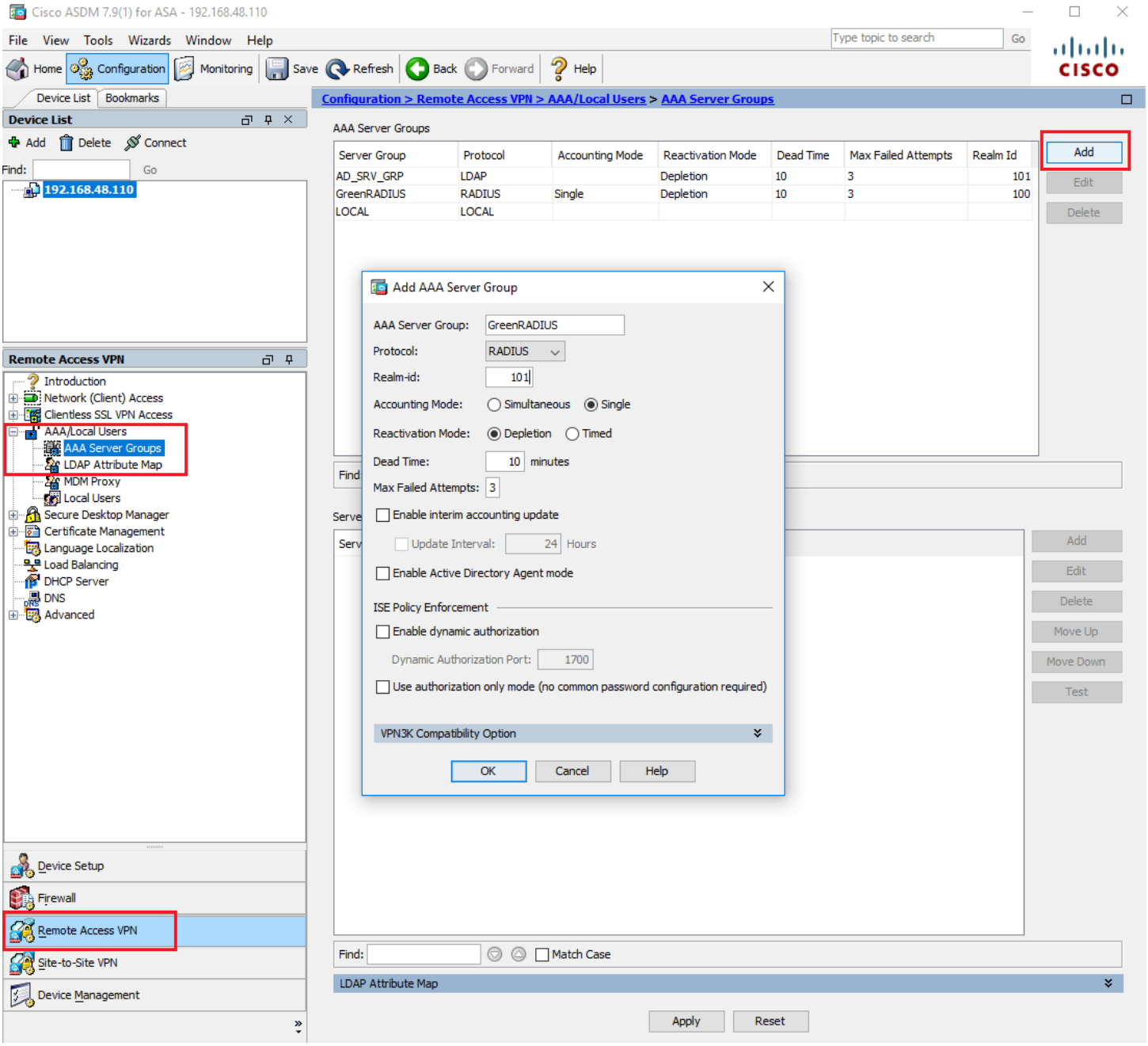
3. Click the “Add” button below the fields to add the Cisco ASA to GreenRADIUS. Once done, the details entered will appear below.



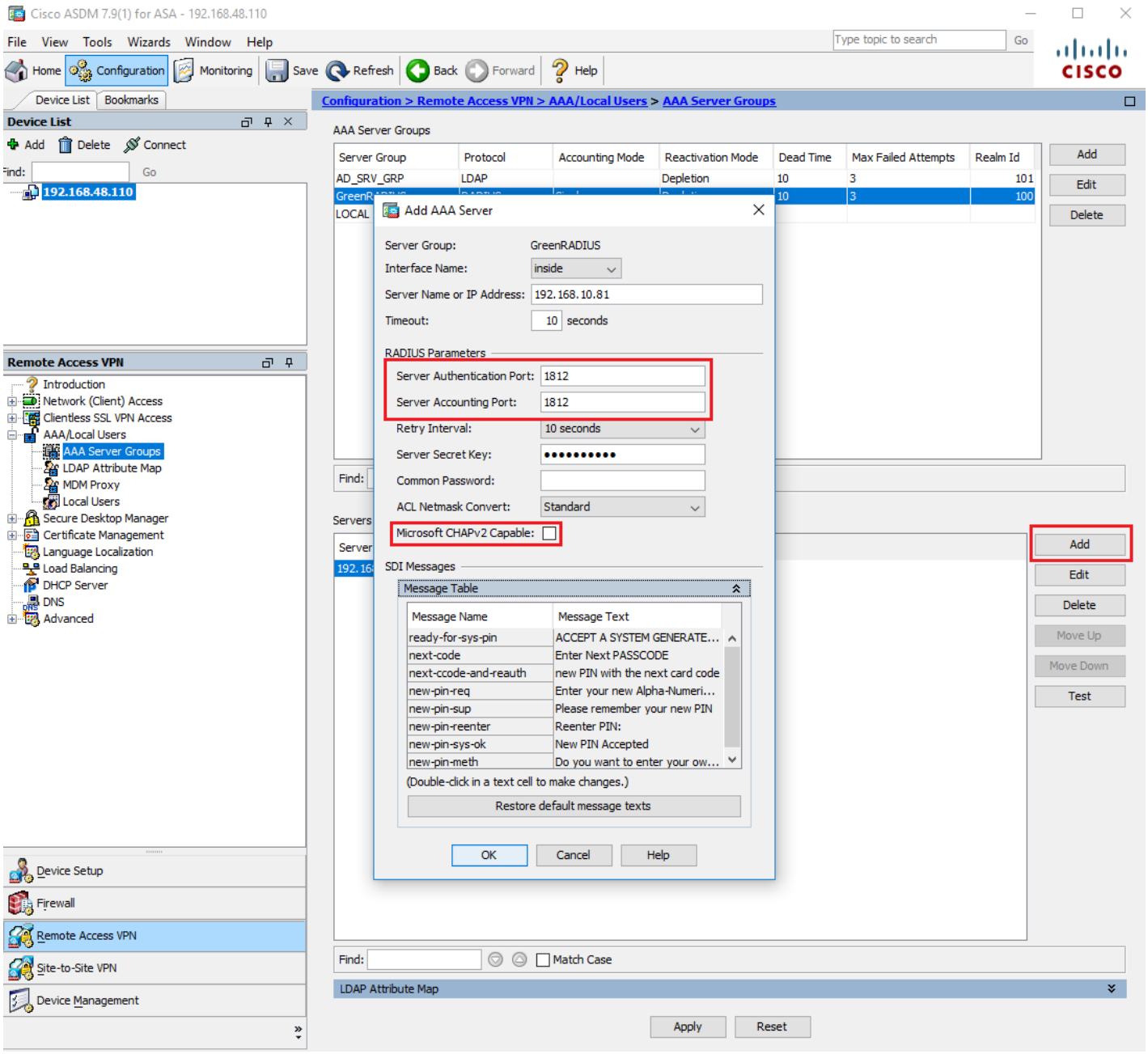
2 Cisco AAA Server Configuration

Before starting, ensure that network interfaces and client profiles are configured correctly.

1. Log in to the Cisco ASDM for ASA.
2. Open the “Configuration” tab and select “**Remote Access VPN**”.
3. Locate “AAA/Local Users” and select “AAA Server Groups”. Click the top right Add button to create a new “GreenRADIUS” RADIUS server group:



4. Select the new “GreenRADIUS” AAA Server Group and click the bottom right Add button. This will open the AAA Server window:



Server Name or IP Address: **greenradius_ip_or_fqdn**

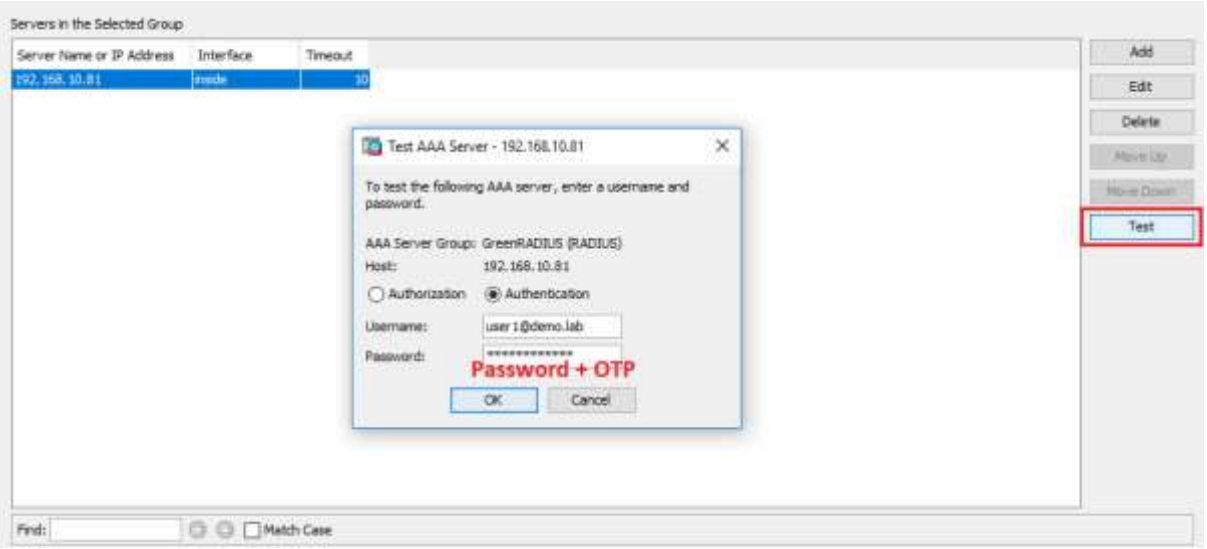
Server Authentication Port: **1812**

Server Accounting Port: **1812**

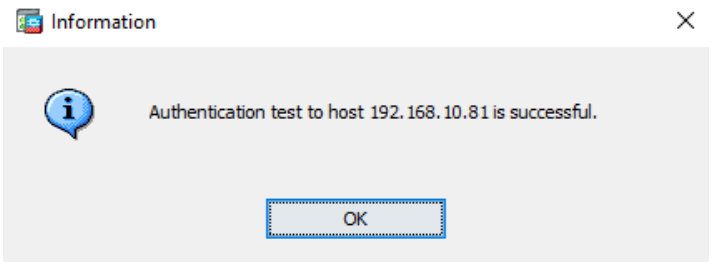
Server Secret Key: **Client Secret** provided in the RADIUS Clients tab on the GreenRADIUS web admin interface (from Step 1.2.2 above).

Microsoft CHAPv2 Capable: **Unchecked**

5. Click OK. Choose “**Test”** to verify the above configuration:



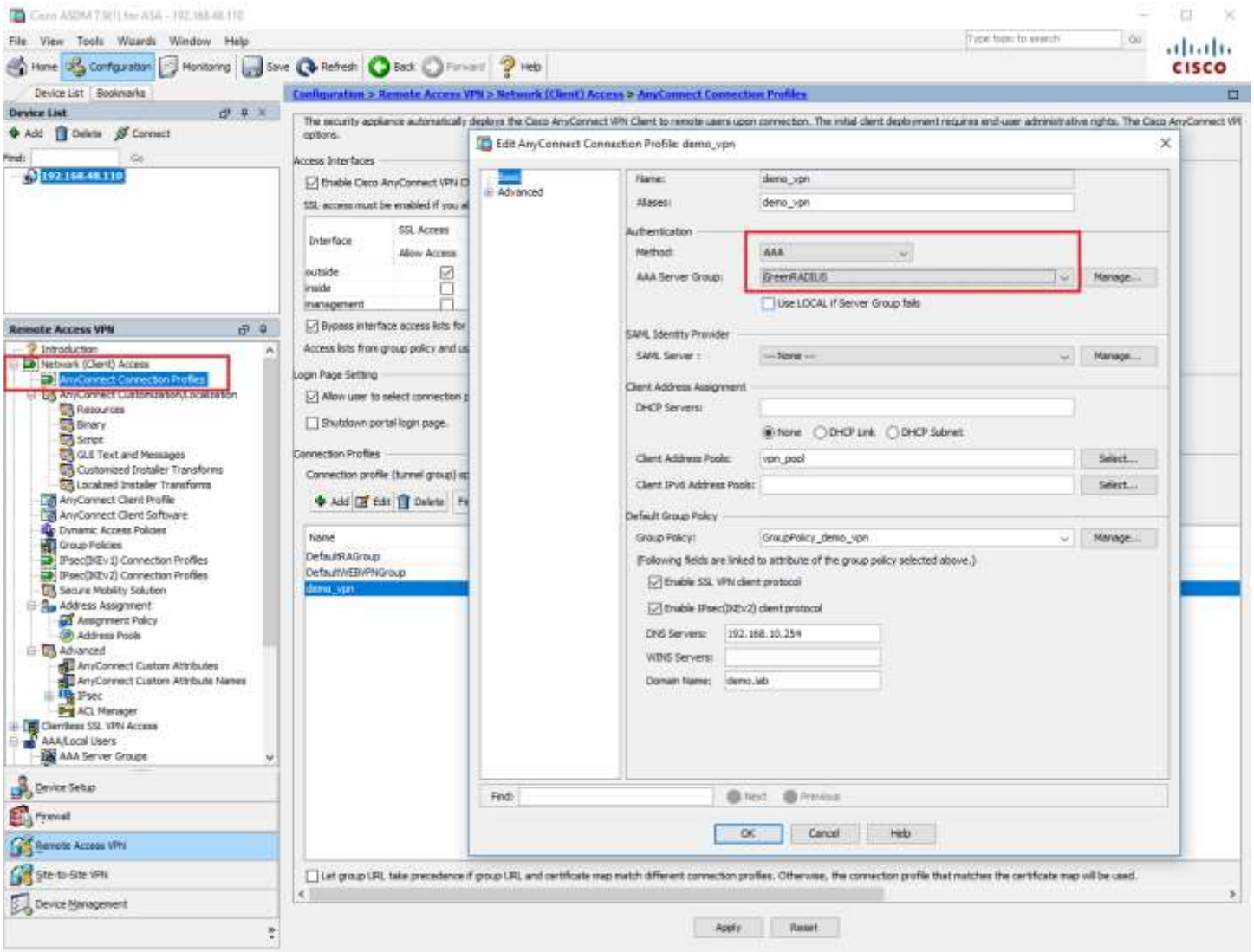
6. Select “Authentication”. Enter the test user’s username and password and append the token’s OTP to the password in the Password field, then press “OK”.



3 Cisco Network Client Access Configuration

1. Locate “Network (Client) Access” on **Remote Access VPN** and select your “Connection Profile”.

2. Under Authentication, choose **Method: AAA** and **AAA Server Group: GreenRADIUS**, then “OK”.



3. We have successfully configured your Cisco ASA Remote Access VPN with GreenRADIUS. Now, just connect from a client machine by appending the token's OTP to the password.