Info from the following: Neno Spasov, bbxie, Nicolas Darchis

https://supportforums.cisco.com/thread/2053236

There are several things that you have to do before the machine authentication can work:

1. Under Users and Identity stores > Active Directory: Make sure: ACS is joined to your domain and you can see the needed groups under Directory Groups
2. Check the box "enable machine authentication"
   Aging time (hours): Once a machine is authenticated this timer starts to tick. Once the time is up the machine would have to be restarted in order for machine authentication to re-occur. (8 or more hours should be fine)
3. Under Access Policies perform the following:
   a. Select Access Services and click on 'Create'
   b. Name it 'Wireless network access' (or whatever you like)
   c. Under 'User Selected Services Type' select Network Access
   d. Under 'Policy Structure' select Identity and Authorization
   e. Click 'Next'
   f. Step 2 - Allowed Protocols select the following:
      i. Process Host Lookup
      ii. Allow PEAP
      iii. Allow EAP-MS-CHAPv2
      iv. Allow Password Change
   g. Click 'Finish'
   h. The following popup will appear, click 'Yes' to accept

   Access Service created successfully. Would you like to modify the Service Selection policy to activate this service?

4. Under 'Service Selection Rules'
   a. 'Customize' (on the bottom right side) ***Optional**
   b. You can choose whatever you want to match, but for this, I will make it simple. Choose only the following:
      i. Protocol
      ii. Device IP Address ***Optional**
   c. Click 'Ok'
   d. Click 'Create'
   e. Name it 'Wireless network access' (or whatever you like)
   f. Click 'Protocol' and match 'Radius'
   g. 'Service' should be the 'Access Service' you created in step #1
   h. Check 'Device IP Address' ***Optional**
   i. Input the ip address of the WLC (Management IP) ***Optional**
   j. Click 'Add v' ***Optional**
   k. Under Results | Service choose the service you created ***Optional**
   l. Click 'Ok'
   m. Click 'Save Changes' on the bottom
5. Under Access Policies | Access Services | <Your new rule>

a. Select 'Identity'
b. Under 'Identity Source' choose AD1
c. Click 'Save Changes' on the bottom

6. Under Access Policies | Access Services | <Your new rule>
   a. Select 'Authorization'
   b. Click 'Customize' (on the bottom right side)
   c. You can choose whatever you want to match, but for this, I will make it simple. Choose only the following:
      i. System:UserNAme
      ii. Was Machine Authenticated
      iii. AD1:ExternalGroups
      iv. Remove Compound Conditions!!!!!
      v. Click 'Ok'
      vi. Click 'Save Changes' on the bottom

7. YOU WILL NEED TO CREATE TWO RULES
   a. RULE #1
      i. Click 'Create' and name the rule if you wish
      ii. Make sure the Status is set to 'Enabled'
      iii. Check 'Systen:UserName'
      iv. The rule should be as follows" 'starts with' input 'host/' without the quotes
      v. Under 'Results' 'Authorization Profiles' click 'Select' and choose 'Permit Access'
      vi. Click 'Ok' and Click 'Ok' again
      vii. This is all for this rule.
      viii. Click 'Ok' on the bottom
   b. RULE #2
      i. Click 'Create' and name the rule if you wish
      ii. Make sure the Status is set to 'Enabled'
      iii. Check 'Was Machine Authenticated'
      iv. The rule should be as follows" '= True'
      v. Check 'AD1:ExternalGroups' and select 'contains any'
      vi. Click on 'Select' and choose the AD user group in which the user resides in
      vii. Under 'Results' 'Authorization Profiles' click 'Select' and choose 'Permit Access'
      viii. That is all for this rule.
      ix. Click 'Ok' on the bottom
   c. DEFAULT Rule
      i. Click 'Default' at the bottom
      ii. Deselect Permit Access and Select Deny Access
      iii. Click 'Ok'
      iv. Click 'Save Changes' on the bottom