If you haven't already done so you'll need to register IAS with Active Directory.

Create a RADIUS Client

First we need to create a RADIUS Client in IAS that will represent our WCS Server. In IAS right click on "RADIUS Clients" and select "New RADIUS Client"

The new RADIUS client wizard will walk you though the process of adding the RADIUS device.

In the "Friendly name" field I used the hostname of the WCS server.

Next, populate the "Client address (IP or DNS)" field with the IP address or DNS name of the WCS Server and then click "Next".

On the following screen select "RADIUS Standard" from the Client-Vendor list. Then enter a shared secret (password) that WCS will use to authenticate to IAS. Confirm your shared secret and click "Finish". Do NOT check the box "Request must contain the Message Authenticator attribute".

Note: Shared secrets are case sensitive.

Create a RADIUS Policy

Now we need to create a Remote Access Policy. We'll begin by defining who has access to WCS. To begin right click on "Remote Access Policy" and select "New Remote Access Policy"

When the New Remote Access Policy Wizard begins click "Next".

Select "Set up a custom policy" under "How do you want to set up this policy?" Then create a name for your policy.
I used "Cisco WCS". Once you've named your policy click "Next".

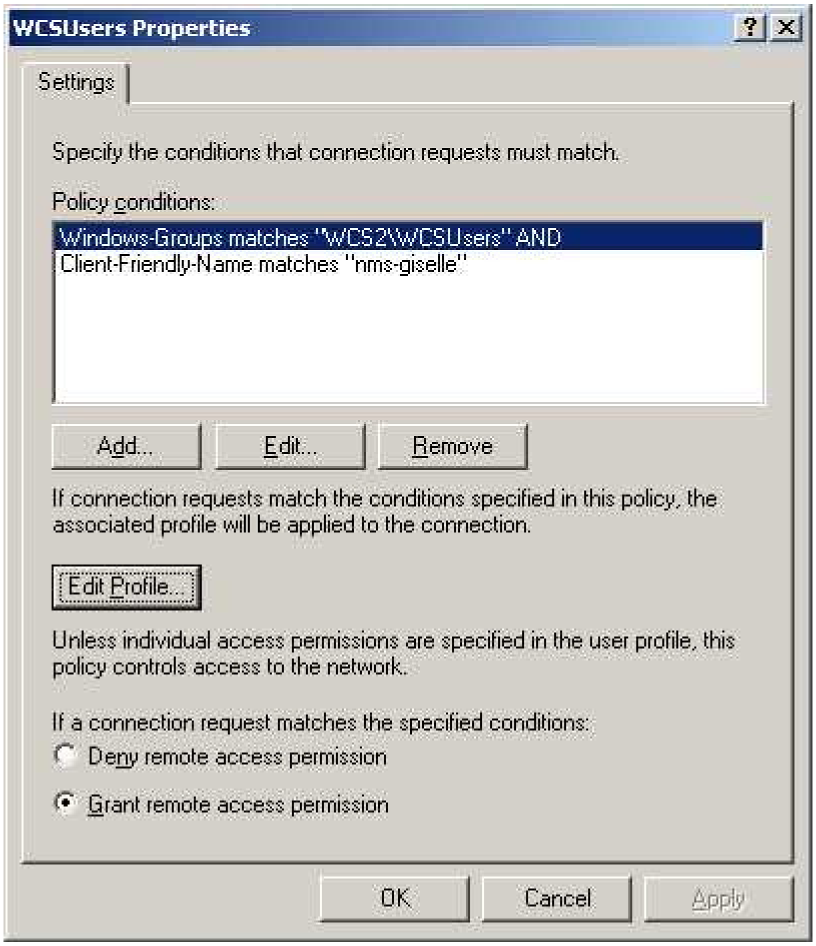
On the Policy Conditions page click "Add" and select "Windows-Groups" and click "Add" again.

In the Groups page click "Add" and select the Active Directory user group you want to have administrative access to WCS.

Once again on the Policy Conditions page click the "Add" button and choose "Client-Friendly-Name" from the list and click "Add".

In the Client-Friendly-Name window type the hostname of the WCS server. This will ensure that this Remote Access Policy only applies to the WCS Server RADIUS client that we defined ealier. When you are done click "OK".

Your Policy conditions should look similar to the image below. If everything looks good then click "Next".



WCSUsers Properties

Settings

Specify the conditions that connection requests must match.

Policy conditions:

Windows-Groups matches "WCS2\WCSUsers" AND
Client-Friendly-Name matches "nms-giselle"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

On the Permissions screen select "Grant remote access permission" and click "Next".

On the Profile page click "Edit Profile" and go to the "Authentication" tab. Check the box labeled "Unencrypted authentication (PAP, SPAP). Uncheck all other boxes.

Next, click on the "Encryption" tab and clear all the checkboxes except "No encryption"

Click on the "Advanced" tab and remove all attributes that are listed, and then click "Add". Select "Vendor-Specific" from the list and click "Add".

Click "Add" Again and the "Mutivalued Attribute Information" window appears. click "Add" one last time to add an attribute value to the list.

In the "Vendor-Specific Attribute Information" click on the vendor list and select "Cisco". Select the radio button "Yes it conforms" and lastly click "Change Attribute".

Here in the Vendor Specific Attribute (VSA) we define the RADIUS response messages sent back to WCS upon a successful authentication.

We begin by changing the "Vendor-assigned attribute number". This number will always be "1" for all WCS VSA(s).

The first "Attribute value" that we'll define is the WCS role that the user who successfully authenticated to RADIUS will have in WCS.
In this case I use WCS Admin. So in the "Attribute value" we enter "Wireless-WCS:role0=Admin" and click "OK".

You must define the role that the authenticated user will be a member of and you must also specifically define the tasks the user can perform on WCS. At this time there are currently ~65 "tasks" within WCS that can be controlled through RADIUS. You must include each task as a VSA that you want your users to have access to in WCS.

Below is a listing of all current WCS tasks and the virtual domain as of version 6.0.181.0 in proper VSA format. They will need to be added individually to grant users logging in to WCS full access.

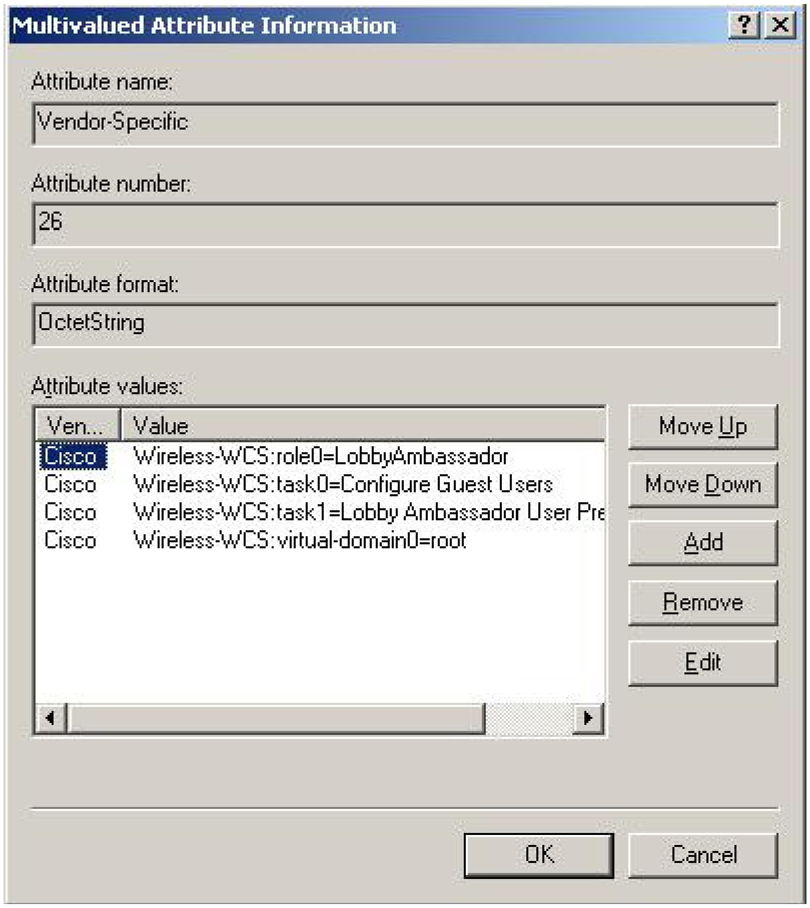
Do not forget the Virtual Domain. If you have only the Root Virtual Domain if you forget to add it you will be dropped in the Root domain. This is not really an issue until you have more than one defined.

```
Wireless-WCS:virtual-domain0=root

Wireless-WCS:role0=Admin
Wireless-WCS:task0=Users and Groups
Wireless-WCS:task1=Virtual Domain Management
Wireless-WCS:task2=Audit Trails
Wireless-WCS:task3=TACACS+ Servers
Wireless-WCS:task4=RADIUS Servers
Wireless-WCS:task5=Logging
Wireless-WCS:task6=License Center
Wireless-WCS:task7=Scheduled Tasks and Data Collection
Wireless-WCS:task8=User Preferences
Wireless-WCS:task9=High Availability Configuration
Wireless-WCS:task10=Health Monitor Details
Wireless-WCS:task11=System Settings
Wireless-WCS:task12=View Alerts and Events
Wireless-WCS:task13=Email Notification
Wireless-WCS:task14=Delete and Clear Alerts
Wireless-WCS:task15=Pick and Unpick Alerts
Wireless-WCS:task16=Ack and Unack Alerts
Wireless-WCS:task17=Configure Ethernet Switch Ports
Wireless-WCS:task18=Configure WIPS Profiles
Wireless-WCS:task19=Global SSID Groups
Wireless-WCS:task20=WIPS Service
Wireless-WCS:task21=Configure Controllers
Wireless-WCS:task22=Configure Templates
Wireless-WCS:task23=Configure Config Groups
Wireless-WCS:task24=Configure Access Points
Wireless-WCS:task25=Configure Lightweight Access Point Templates
Wireless-WCS:task26=Configure Autonomous Access Point Templates
Wireless-WCS:task27=Scheduled Configuration Tasks
```

```
Wireless-WCS:task28=Migration Templates
Wireless-WCS:task29=Configure Choke Points
Wireless-WCS:task30=Configure Location Sensors
Wireless-WCS:task31=Configure Spectrum Experts
Wireless-WCS:task32=Configure ACS View Servers
Wireless-WCS:task33=Configure Ethernet Switches
Wireless-WCS:task34=Auto Provisioning
Wireless-WCS:task35=Monitor Controllers
Wireless-WCS:task36=Monitor Access Points
Wireless-WCS:task37=Monitor Clients
Wireless-WCS:task38=Monitor Tags
Wireless-WCS:task39=Monitor Security
Wireless-WCS:task40=Monitor Chokepoints
Wireless-WCS:task41=Monitor Location Sensors
Wireless-WCS:task42=Monitor Spectrum Experts
Wireless-WCS:task43=Interferers Search
Wireless-WCS:task44=RRM Dashboard
Wireless-WCS:task45=Config Audit Dashboard
Wireless-WCS:task46=Mesh Reports
Wireless-WCS:task47=Client Reports
Wireless-WCS:task48=Device Reports
Wireless-WCS:task49=Performance Reports
Wireless-WCS:task50=Security Reports
Wireless-WCS:task51=Network Summary Reports
Wireless-WCS:task52=Compliance Reports
Wireless-WCS:task53=Guest Reports
Wireless-WCS:task54=Voice Audit Report
Wireless-WCS:task55=Report Launch Pad
Wireless-WCS:task56=Run Reports List
Wireless-WCS:task57=Saved Reports List
Wireless-WCS:task58=Report Run History
Wireless-WCS:task59=Configure Guest Users
Wireless-WCS:task60=Maps Read Only
Wireless-WCS:task61=Maps Read Write
Wireless-WCS:task62=Client Location
Wireless-WCS:task63=Rogue Location
Wireless-WCS:task64=Planning Mode
```

When you're done entering all the tasks you want your users to have access to as VSA's in IAS, your Multivalued Attribute Information window should look similar to the following.



Multivalued Attribute Information

Attribute name: Vendor-Specific

Attribute number: 26

Attribute format: OctetString

Attribute values:

Ven...	Value
Cisco	Wireless-WCS:role0=LobbyAmbassador
Cisco	Wireless-WCS:task0=Configure Guest Users
Cisco	Wireless-WCS:task1=Lobby Ambassador User Pre
Cisco	Wireless-WCS:virtual-domain0=root

We've finally completed the configuration of IAS. Click "OK" on each open window to confirm your changes until you're back at the main IAS MMC.

Configure WCS

Now we need to configure WCS to use the RADIUS server as its method of authentication.

We begin by accessing the web interface of WCS and logging in as the WCS administrator. Click Administration > AAA from the top navigation bar. Then select Radius from the menu on the left. On the pull-down choose Add RADIUS Server and click GO.

In the fields enter the Server Address and Shared Secret from the RADIUS server that we defined earlier in the "Create a RADIUS Client". The other fields can usually be left default unless you changed the Authentication Port. Then click "Submit"

Once the RADIUS servers are defined in WCS we need to enable RADIUS authentication. Click on "AAA Mode" from the menu on the left. Select the "RADIUS" radio button and ensure "Enable fallback to Local" on auth failure or no server response is checked so we don't get locked out of WCS if the RADIUS server was to become unavailable.

When you're done click "OK".

From here you should logout and test your RADIUS authentication. Provided that all the steps were followed correctly, you should be able to login successfully.

To debug the authentication/authorization go to Administration > Logging and only check the Configuration and General modules. Change the message level to Trace and click submit. Try to log in as the test user. Go back to Administration > Logging and click Download to get the logs. You will be looking for something similar to this:

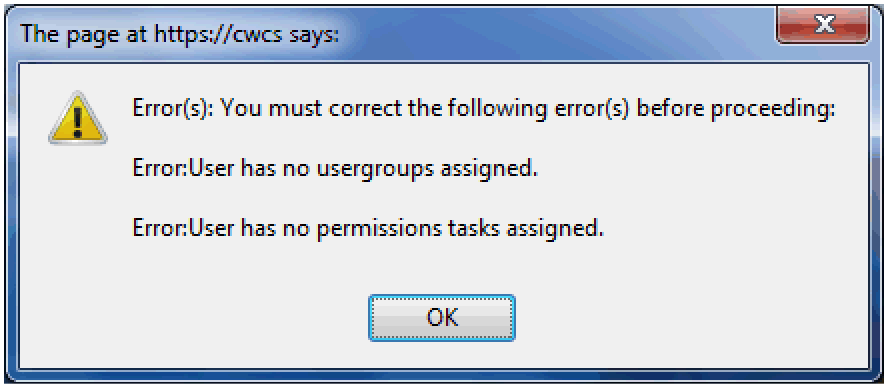
```
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Creating
datagram socket   - To Server:  172.18.123.18  - For User:  WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Building
Access Request Packet  - To Server:  172.18.123.18  - For User:  WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Building and
sending Access Request Datagram  - To Server:  172.18.123.18  - For User:
WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Receiving
Access Response Datagram  - From Server:  172.18.123.18  - For User:
WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Validating
Access Response Authenticator field  - From Server:  172.18.123.18  - For
User:  WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule]  WCSRoot
successfully authenticated for server 172.18.123.18
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS+ AAAModule]
Disconnecting from datagram socket  - From Server:  172.18.123.18  - For
User:  WCSRoot
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Processing
Cisco vendor custom attributes:
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] adding role:
role0 = LobbyAmbassador
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] adding task:
task0 = Configure Guest Users
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] adding task:
task1 = Lobby Ambassador User Preferences
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] adding
virtual domain: virtual-domain0 = root
 4/26/10 13:34:27.141 TRACE[general] [34] [RADIUS AAAModule] Total
permissions for user WCSRoot : tasks  2 : roles  1 : virtual-domains  1
 4/26/10 13:34:27.156 TRACE[config] [34] Adding object AuditTrail#0
(AuditTrail)
 4/26/10 13:34:27.156 TRACE[general] [34] WCSRoot  :  Login succeeded ?
true
```

If you have not defined the VSAs correctly you may see this:

```
 4/26/10 11:13:01.147 TRACE[general] [26] [RADIUS AAAModule] Creating
datagram socket   - To Server:  10.19.75.128  - For User:  c05lc
 4/26/10 11:13:01.147 TRACE[general] [26] [RADIUS AAAModule] Building
Access Request Packet  - To Server:  10.19.75.128  - For User:  c05lc
```

```
 4/26/10 11:13:01.147 TRACE[general] [26] [RADIUS AAAModule] Building and
sending Access Request Datagram  - To Server:  10.19.75.128  - For User:
c05lc
 4/26/10 11:13:01.147 TRACE[general] [26] [RADIUS AAAModule] Receiving
Access Response Datagram  - From Server:  10.19.75.128  - For User:
c05lc
 4/26/10 11:13:01.303 TRACE[general] [58] Acquiring poll sequence lock
Device Status
 4/26/10 11:13:01.303 TRACE[general] [58] Acquired poll sequence lock
Device Status
 4/26/10 11:13:01.538 TRACE[general] [26] [RADIUS AAAModule] Validating
Access Response Authenticator field  - From Server:  10.19.75.128  - For
User:  c05lc
 4/26/10 11:13:01.538 TRACE[general] [26] [RADIUS AAAModule]  c05lc
successfully authenticated for server 10.19.75.128
 4/26/10 11:13:01.538 TRACE[general] [26] [RADIUS+ AAAModule]
Disconnecting from datagram socket  - From Server:  10.19.75.128  - For
User:  c05lc
 4/26/10 11:13:01.538 TRACE[general] [26] [RADIUS AAAModule] Processing
Cisco vendor custom attributes:
 4/26/10 11:13:01.538 TRACE[general] [26] [RADIUS AAAModule] No
authorization information for this user
 4/26/10 11:13:01.538 ERROR[general] [26] [AuthenticationAction] User has
no usergroups/roles assigned. Username= c05lc
 4/26/10 11:13:01.538 ERROR[general] [26] [AuthenticationAction] User has
no tasks/permissions assigned. Username= c05lc
```

Here is an image of the error popup that accompanies the above failure:



The page at https://cwcs says:

Error(s): You must correct the following error(s) before proceeding:

Error:User has no usergroups assigned.

Error:User has no permissions tasks assigned.