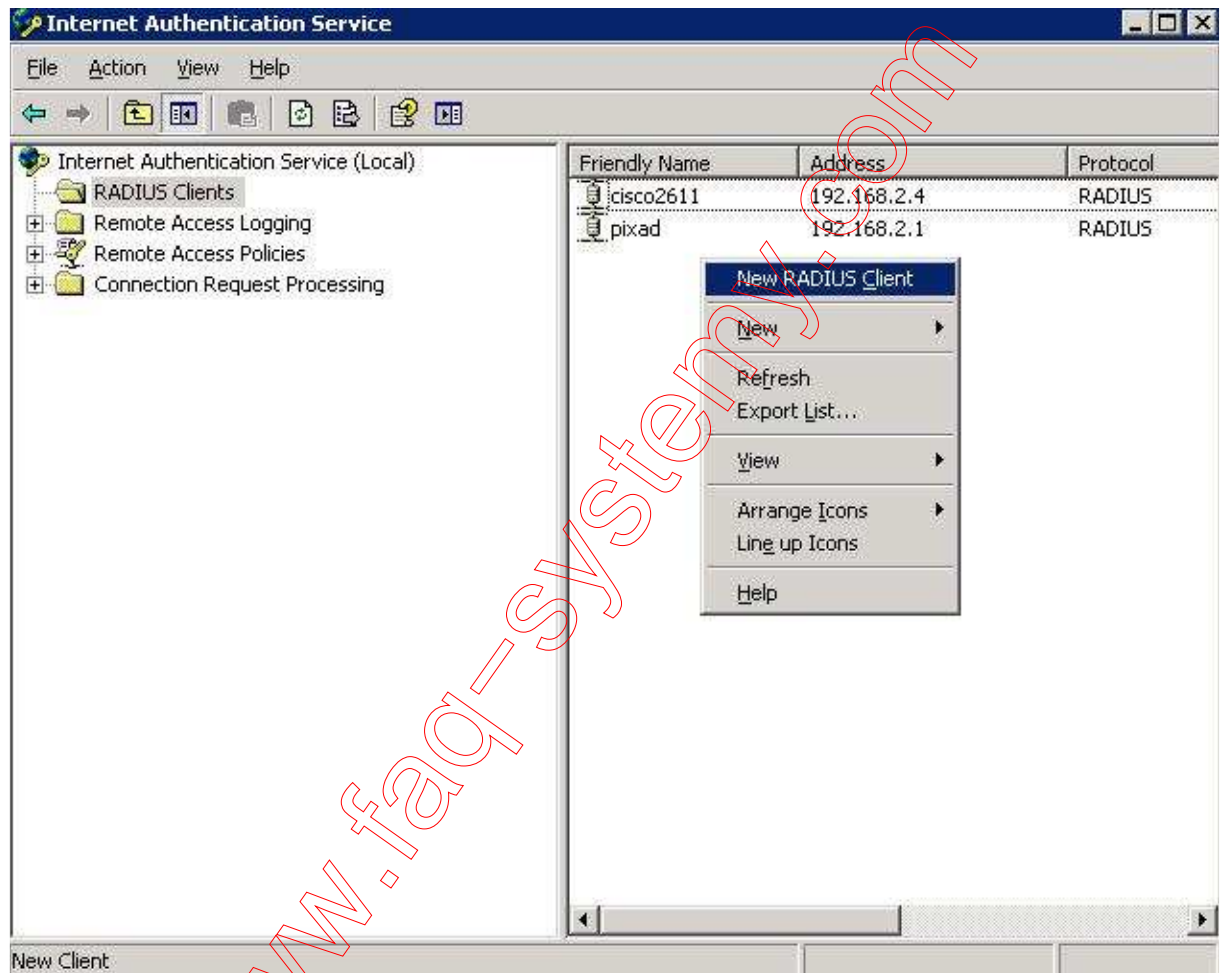


Radius authentication and authorization(exec) for admin access– Cisco AP1131 using web.

1. Create Radius Client



New RADIUS Client [X]

Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

< Back

New RADIUS Client [X]

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:

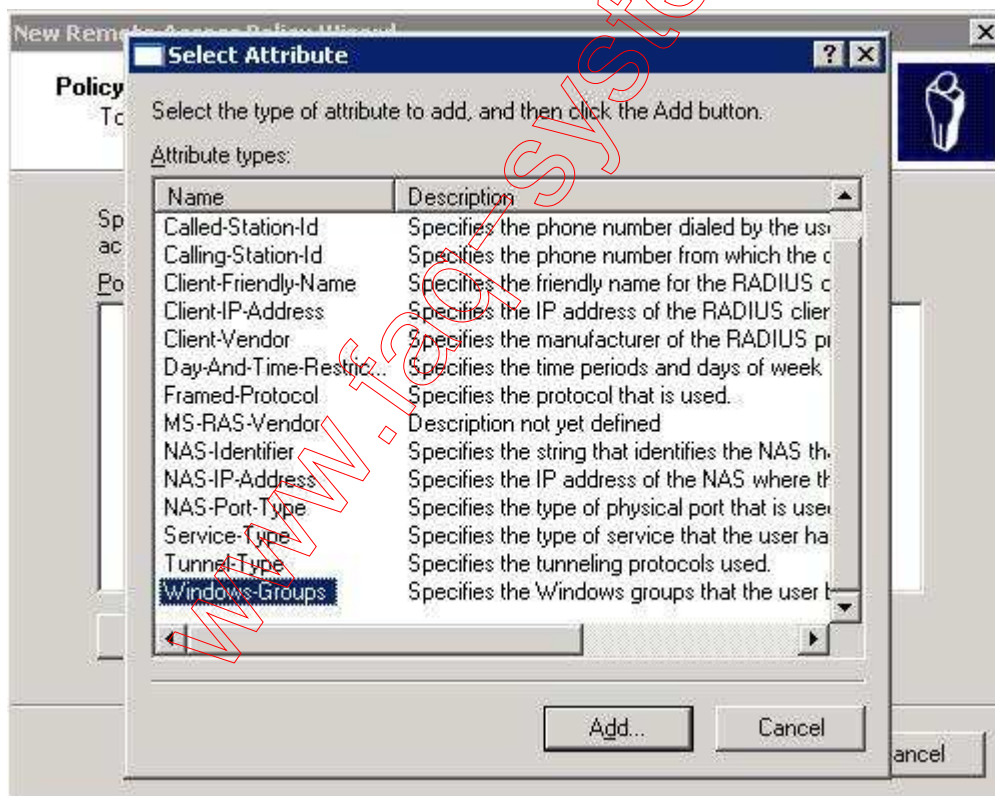
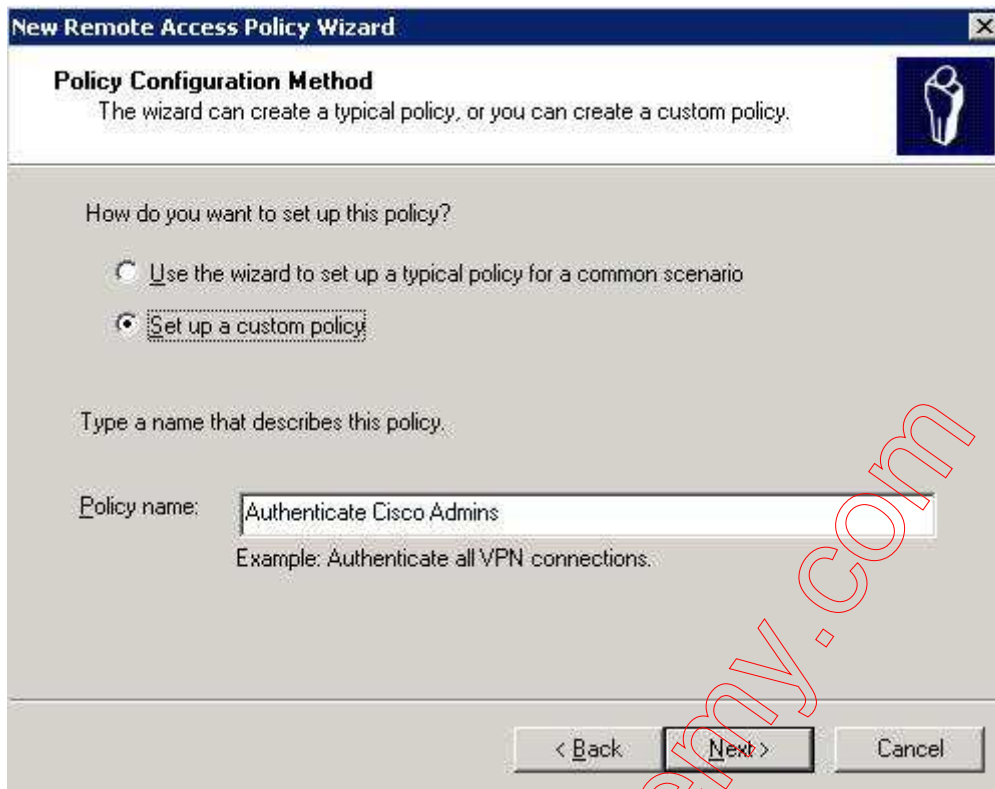
Shared secret:

Confirm shared secret:

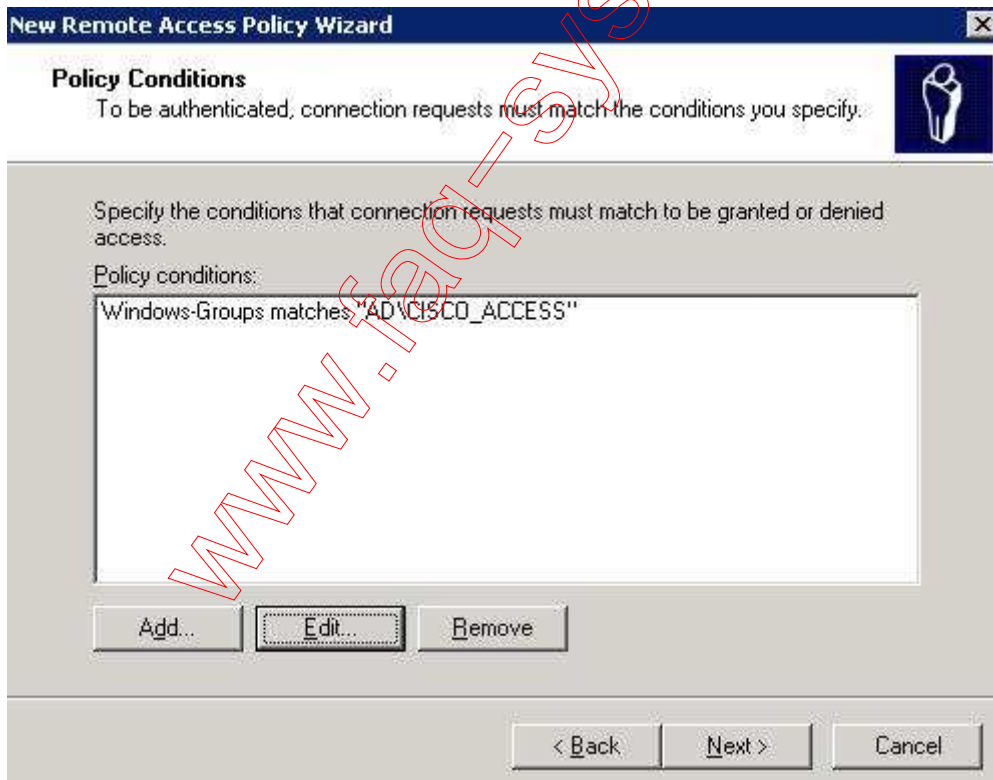
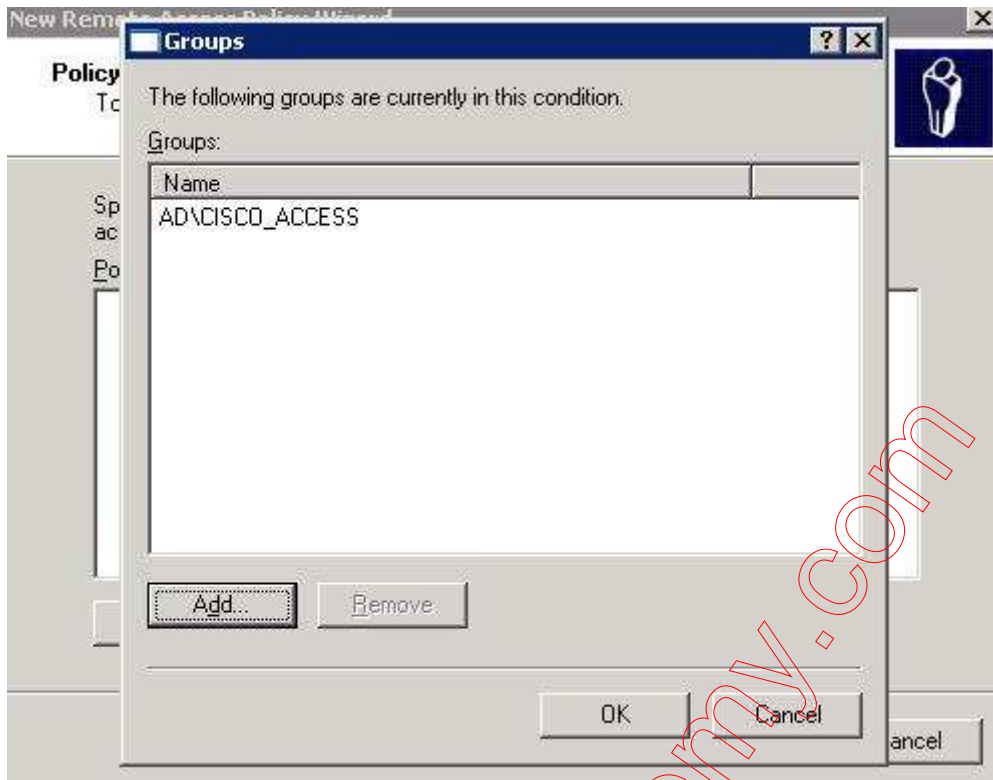
Request must contain the Message Authenticator attribute

< Back Cancel

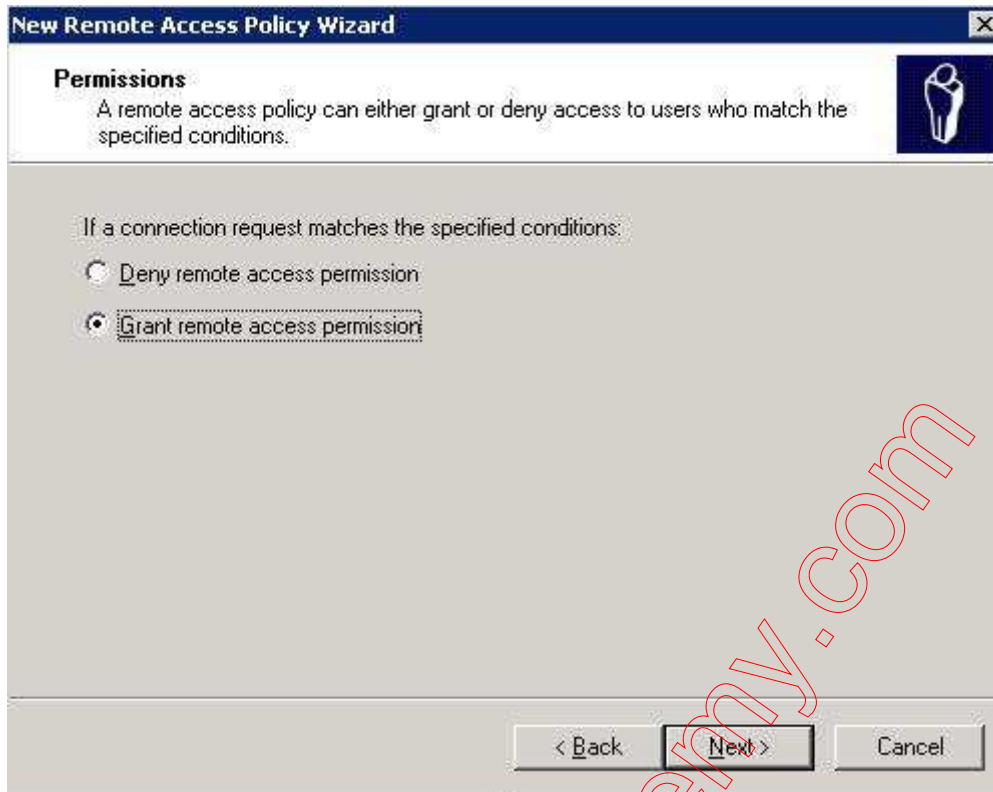
2. Create remote access policy



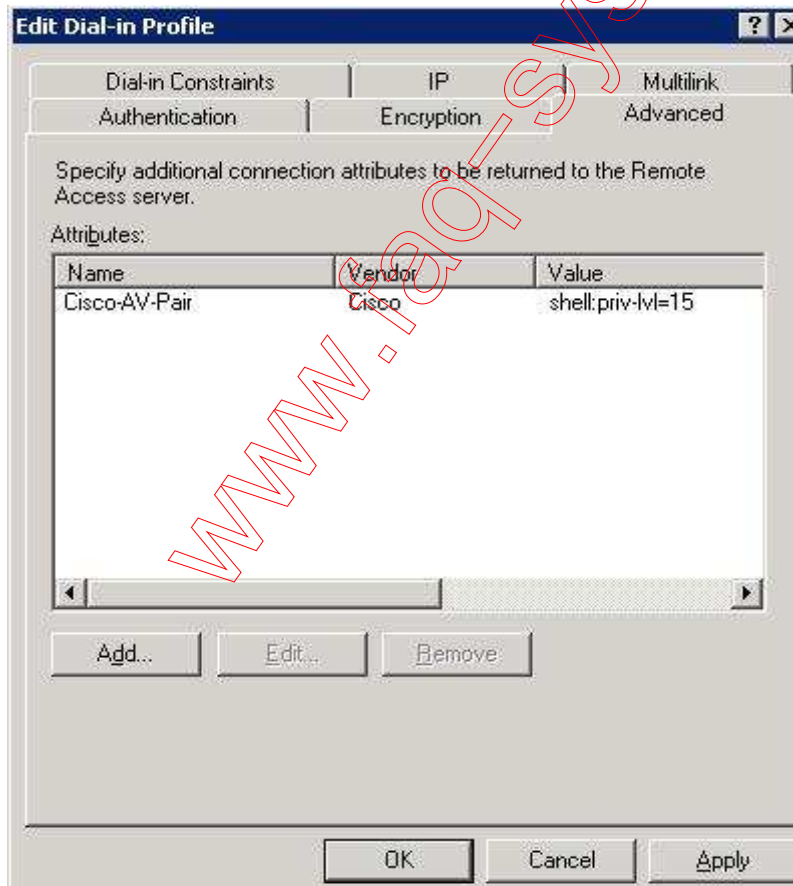
Add active directory group



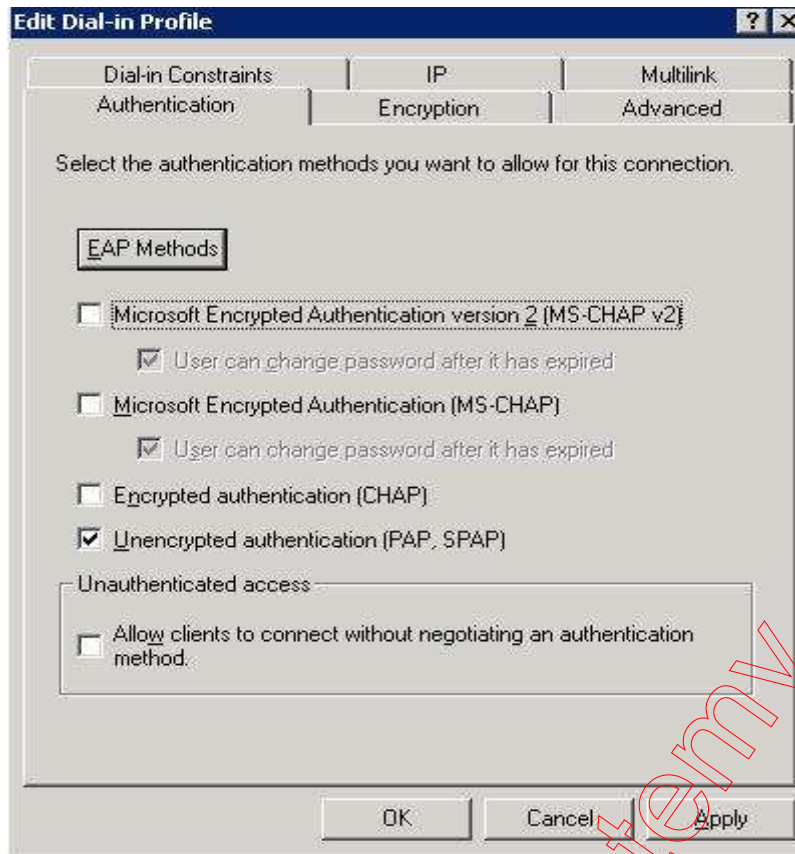
Next



Choose “Grant....” and next and Edit Profile
On Advanced tab remove attributes and add new Cisco-AV-Pair



On “Authentication” tab choose only “(PAP,SPAP).”



Next and finish.

3. Order policy in proper place and remember about policy which forbid everything else

4. Create Radius server(s) for admin authentication

CISCO Cisco Aironet 1130AG Series Access Point

SERVER MANAGER GLOBAL PROPERTIES

Hostname ap ap uptime is 6 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

RADIUS

< NEW >
192.168.2.2

Delete

Server: (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Apply Cancel

5. Set up "Admin Authentication (RADIUS)"

SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

RADIUS

< NEW >
192.168.2.2

Delete

Server: (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: < NONE >	Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >	Priority 3: < NONE >

Admin Authentication (RADIUS)

Priority 1:

Priority 2: < NONE >

Priority 3: < NONE >

Admin Authentication (TACACS+)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Apply Cancel

6. Select authentication method

CISCO Cisco Aironet 1130AG Series Access Point ap uptime is 24 minutes

Hostname **ap**

Security: Admin Access

Administrator Authenticated by:

- Default Authentication (Global Password)
- Local User List Only (Individual Passwords)
- Authentication Server Only
- Authentication Server if not found in Local List
- Local List if no response from Authentication Server

Authentication Cache:

Enable Authentication Server Caching

dzbanek

www.faq-systemy.com