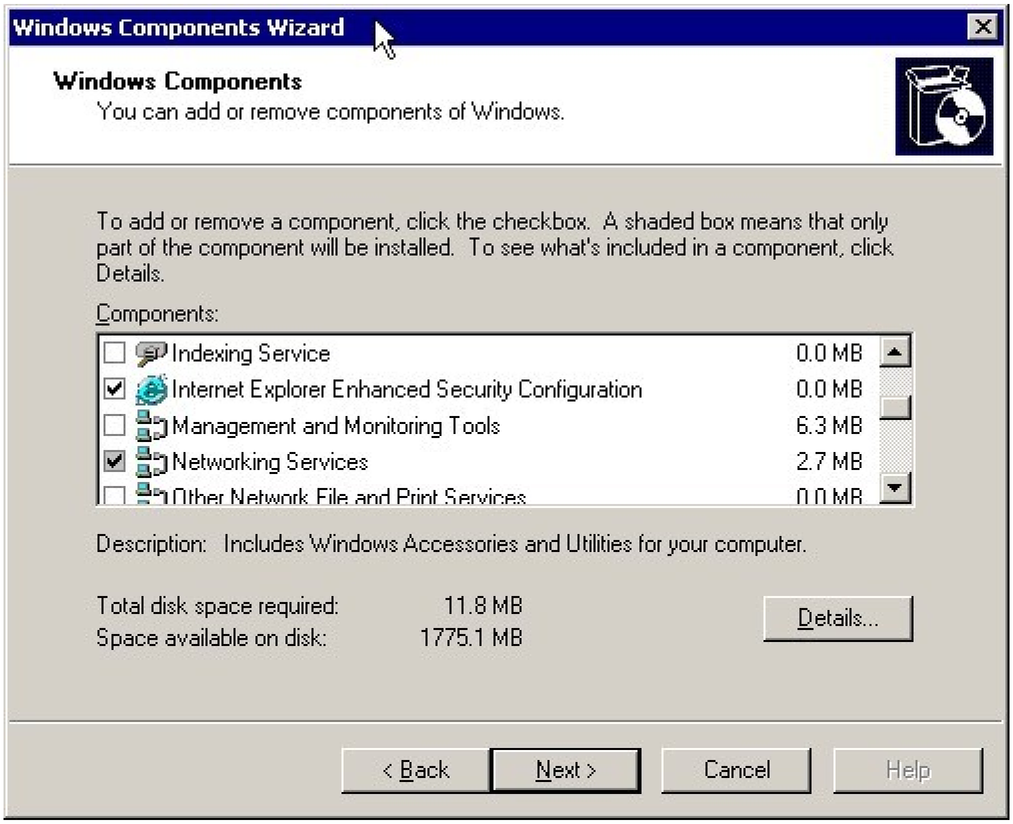
Table of Contents

Using Microsoft Internet Authentication Service server as a Radius server

Internet Authentication Service (IAS) in Microsoft Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. You can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. In the Enterprise and Datacente Edition of Windows Server 2003 these limitations are not existing.

Installing IAS

Windows Server 2003 does not install IAS in the default installation. The IAS must be installed separately later from windows components under the **Networking Services**:



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

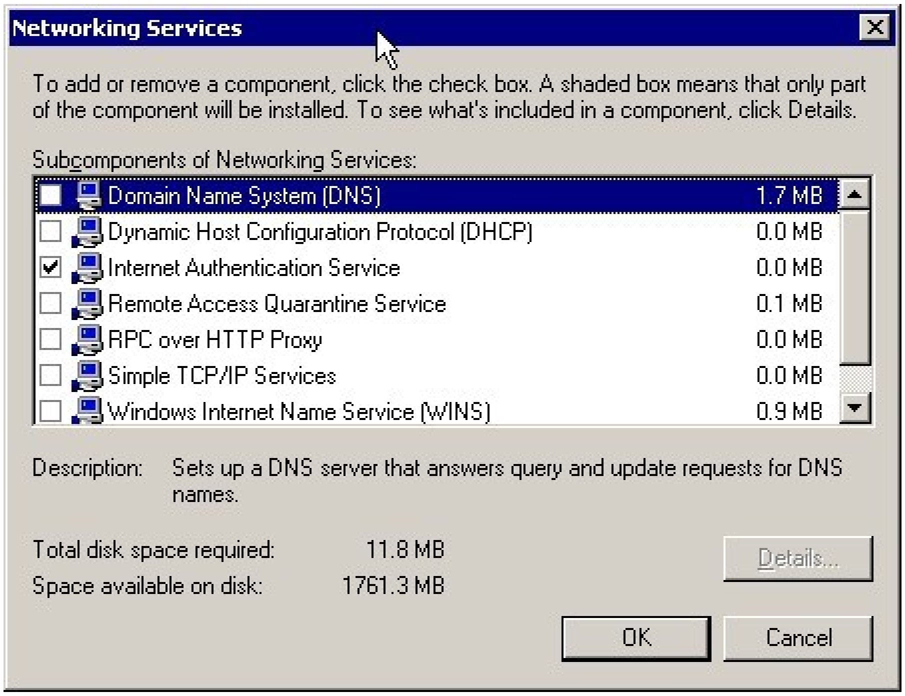
□	Indexing Service	0.0 MB
☑	Internet Explorer Enhanced Security Configuration	0.0 MB
□	Management and Monitoring Tools	6.3 MB
☑	Networking Services	2.7 MB
□	Other Network File and Print Services	0.0 MB

Description: Includes Windows Accessories and Utilities for your computer.

Total disk space required: 11.8 MB

Space available on disk: 1775.1 MB

The **Internet Authentication Service** must be selected:



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

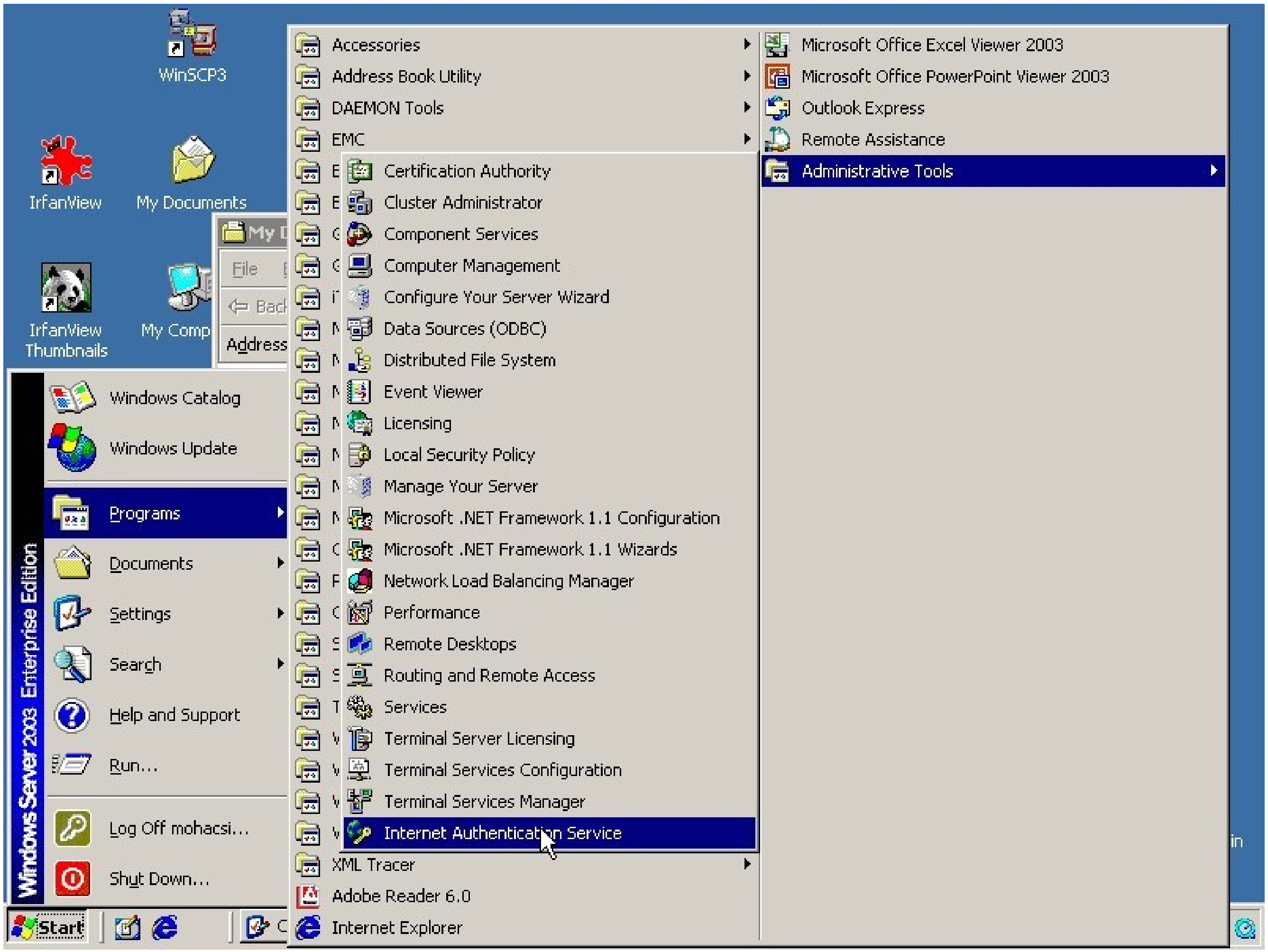
□	Domain Name System (DNS)	1.7 MB
□	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
□	Remote Access Quarantine Service	0.1 MB
□	RPC over HTTP Proxy	0.0 MB
□	Simple TCP/IP Services	0.0 MB
□	Windows Internet Name Service (WINS)	0.9 MB

Description: Sets up a DNS server that answers query and update requests for DNS names.

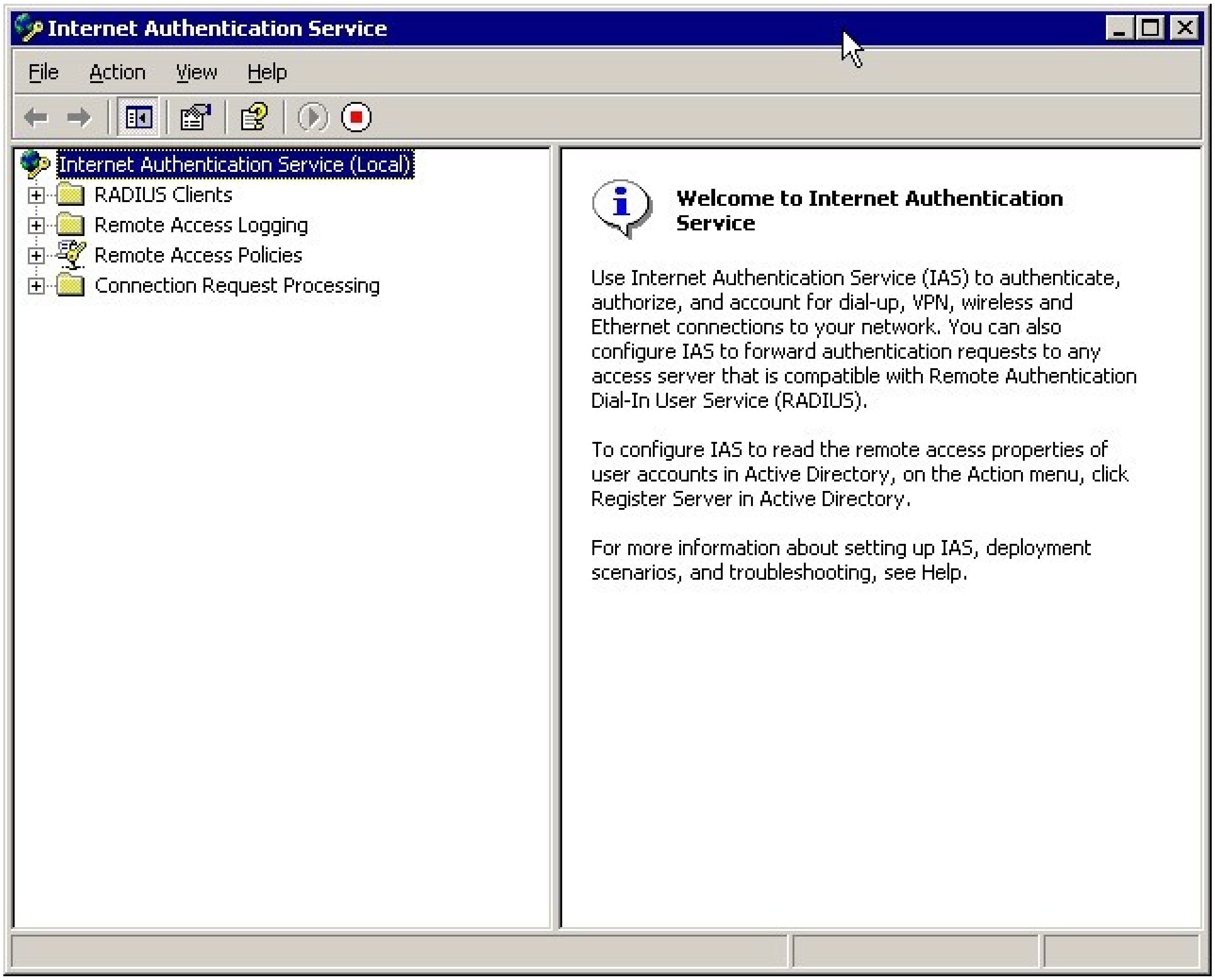
Total disk space required: 11.8 MB

Space available on disk: 1761.3 MB

And wait for the installation to be finished. The IAS administrative console can be found under the **Administrative Tools:**



Clicking the Internet Authentication Service menu the IAS console will start:


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

Welcome to Internet Authentication Service

Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).

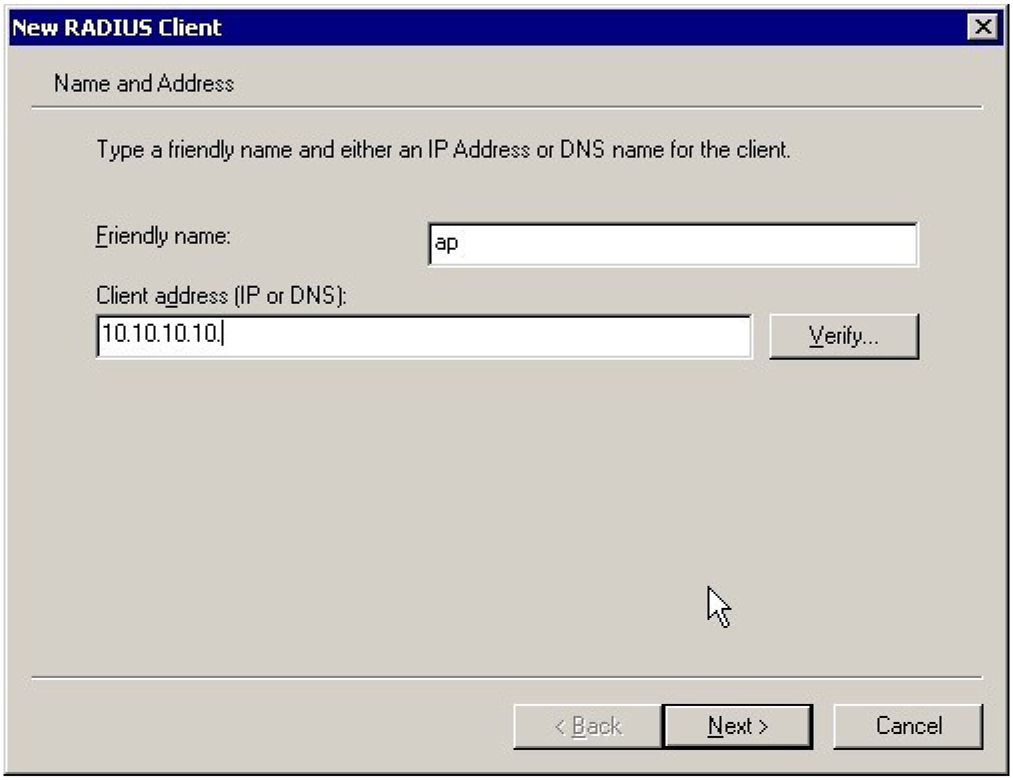
To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.

For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

Configuring IAS to act as a university radius server in Eduroam hierarchy

Configuring IAS for accesspoints and upstream proxies

For each access point and upstream proxies (i.e national eduroam Radius server) the Radius Clients parameter must be configured. When you add a new access point a wizard will start asking the name and IP address of the radius client (i.e. Access Point, switch, or upstream radius proxy).



New RADIUS Client

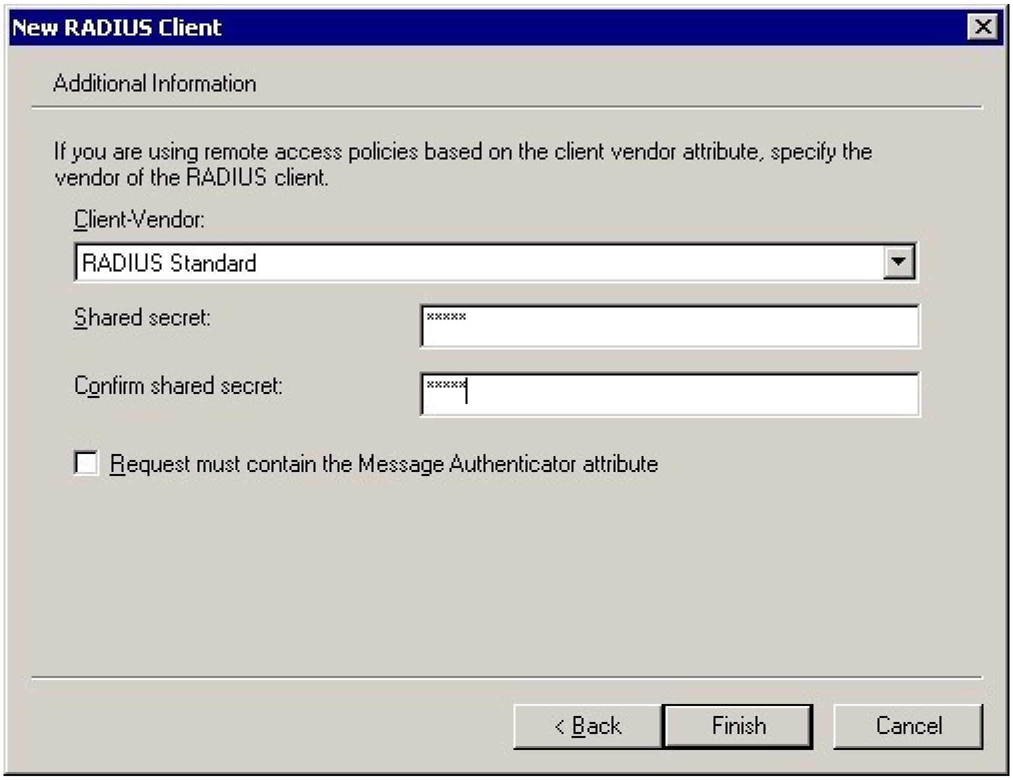
Name and Address

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

Friendly name: ap

Client address (IP or DNS): 10.10.10.10

Then you have to specify the shared secret between the radius client and your radius server (IAS):



New RADIUS Client

Additional Information

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

Client-Vendor: RADIUS Standard

Shared secret: *****

Confirm shared secret: *****

□ Request must contain the Message Authenticator attribute

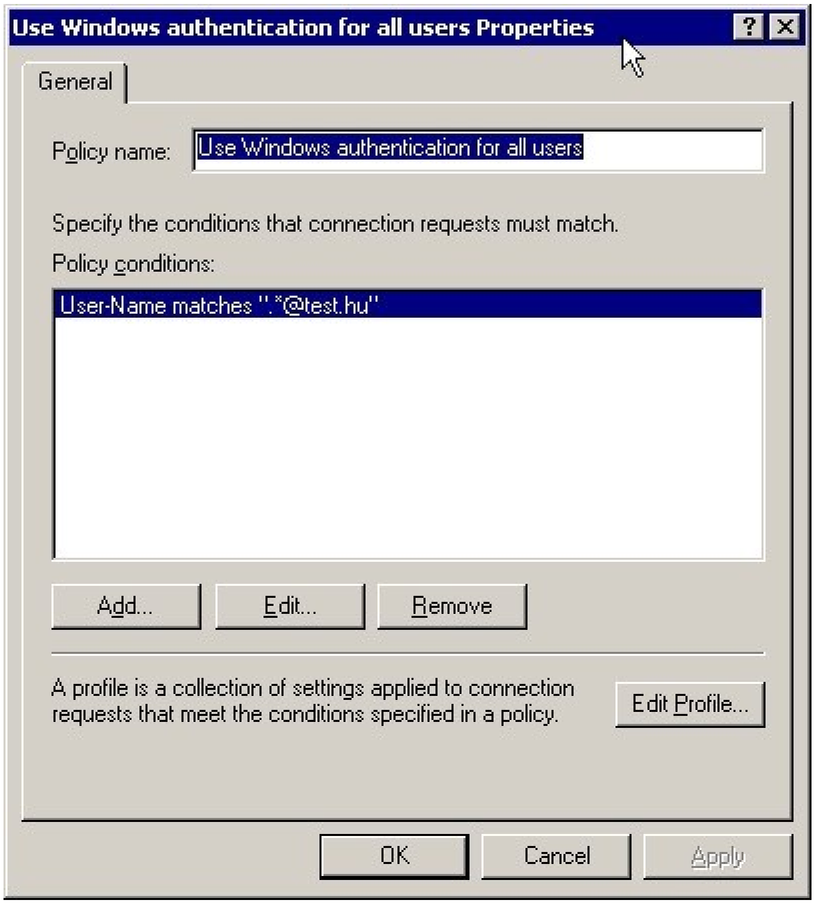
You can select various vendor of Radius clients, but most of the case you should use **Radius Standard.**

Configuring Connection Request Processing Policy

The realm processing should be heavily configured to be properly used in the Eduroam hierarchy. First you have to configure a policy to catch local realms, then configure policy that forward rest of the request to your upstream proxy server.

Configuring policy for local realm

You should configure a Connection Request Processing Policy, that captures all the User-Name-s that is used for access to local realms with policy condition “.*@ yourrealm.cc”.



Use Windows authentication for all users Properties

Policy name: Use Windows authentication for all users

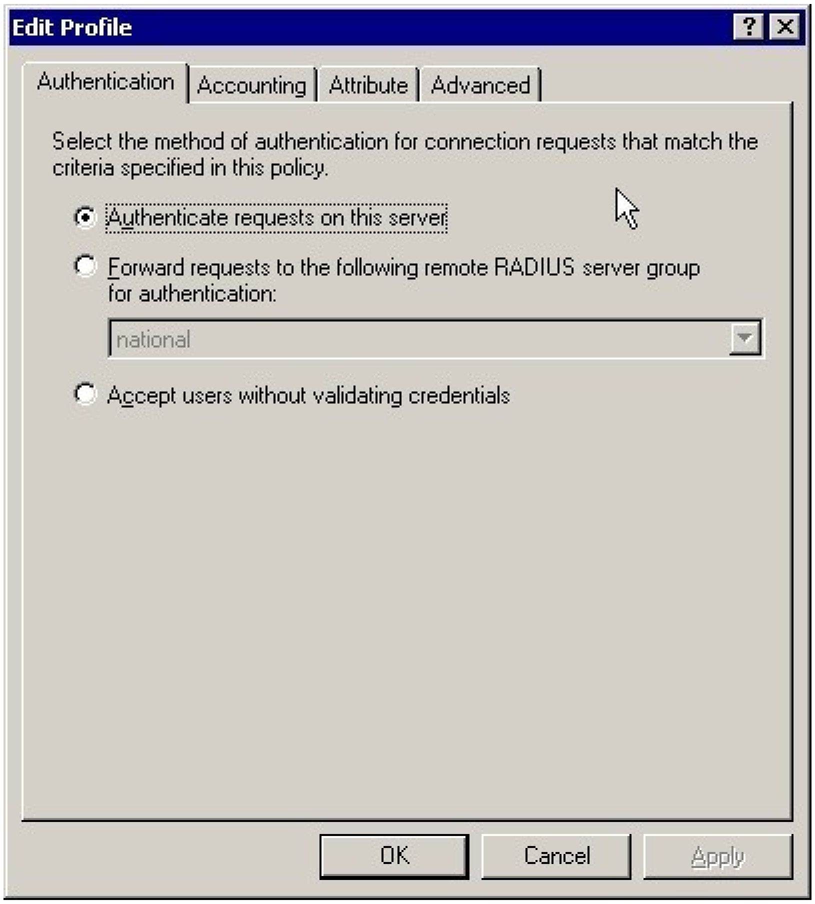
Specify the conditions that connection requests must match.

Policy conditions:

User-Name matches ".*@test.hu"

A profile is a collection of settings applied to connection requests that meet the conditions specified in a policy.

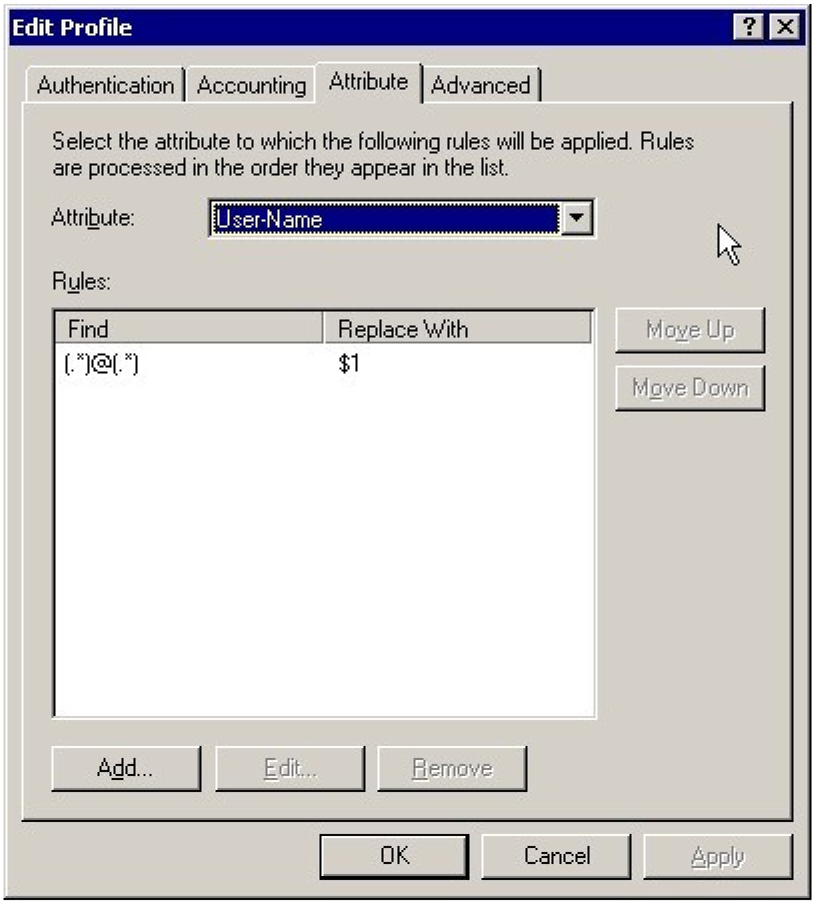
In this case the profile will be more complicated. The authentication should happen on the local server:



Select the method of authentication for connection requests that match the criteria specified in this policy.

- ● Authenticate requests on this server
- ○ Forward requests to the following remote RADIUS server group for authentication:
  national
- ○ Accept users without validating credentials

But the Radius attributes must be processed. In the case of matching realm name the realm name must be stripped off:



Select the attribute to which the following rules will be applied. Rules are processed in the order they appear in the list.

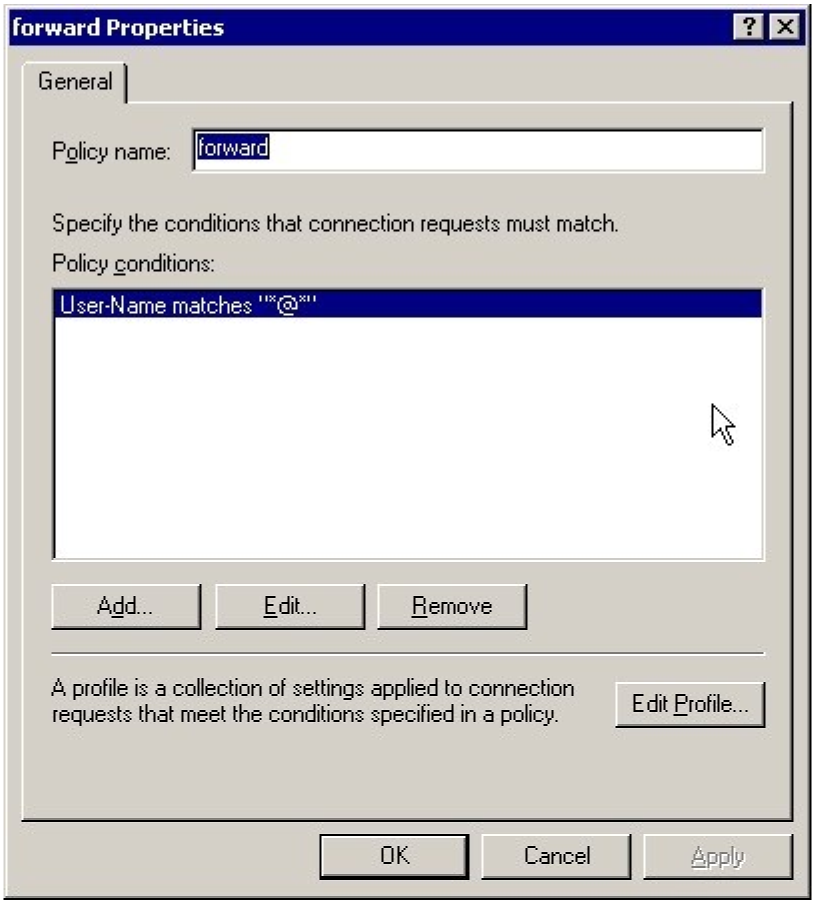
Attribute: User-Name

Rules:

Find	Replace With
(.*)@(.*)	$1

Configuring policy for upstream radius proxy server

You should configure a Connection Request Processing Policy, that captures all the User-Name-s that is potentially used for roaming with policy condition “.*@ .*”.



forward Properties

General

Policy name: forward

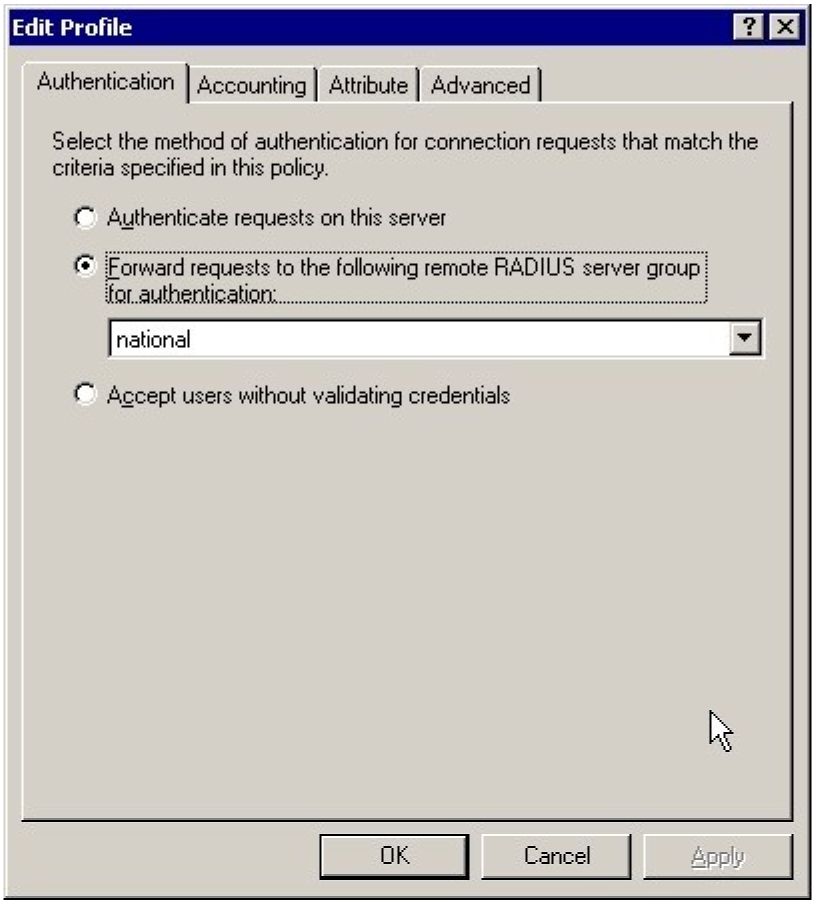
Specify the conditions that connection requests must match.

Policy conditions:

User-Name matches "*@*"

A profile is a collection of settings applied to connection requests that meet the conditions specified in a policy.

Then you should edit the profile to be forwarded to the national proxy server:



Select the method of authentication for connection requests that match the criteria specified in this policy.

○ Authenticate requests on this server

● Forward requests to the following remote RADIUS server group for authentication:

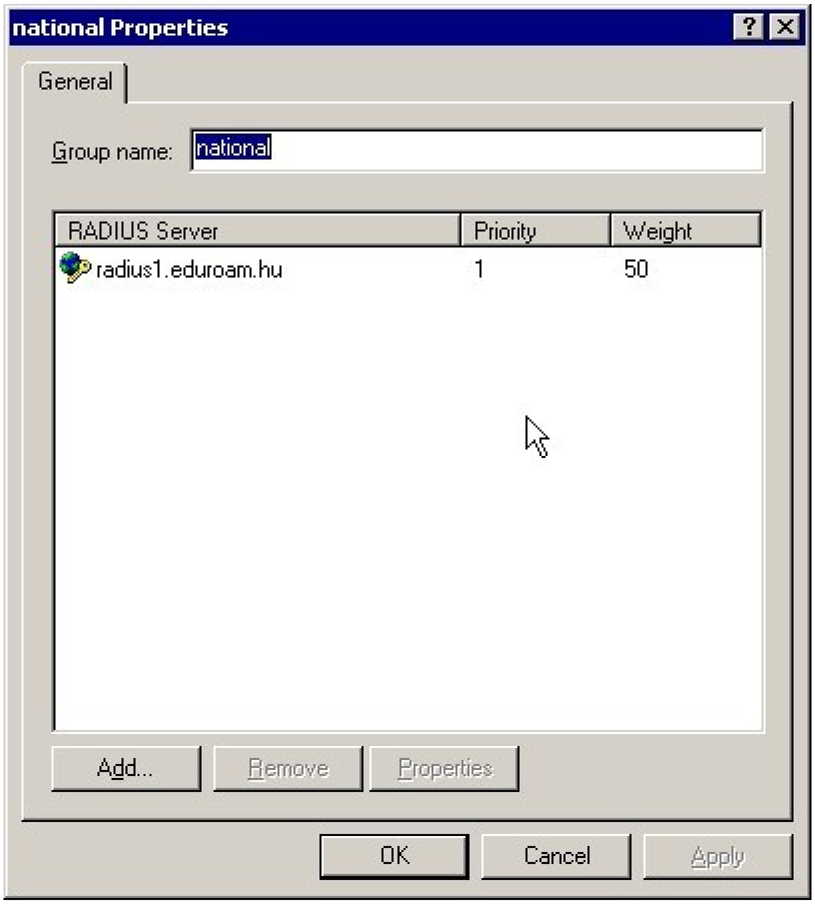
national

○ Accept users without validating credentials

You should configure first the remote radius server group first in order to be able to select from the list.

Configuring remote Radius servers

The national radius proxy server must be added to the remote radius server:

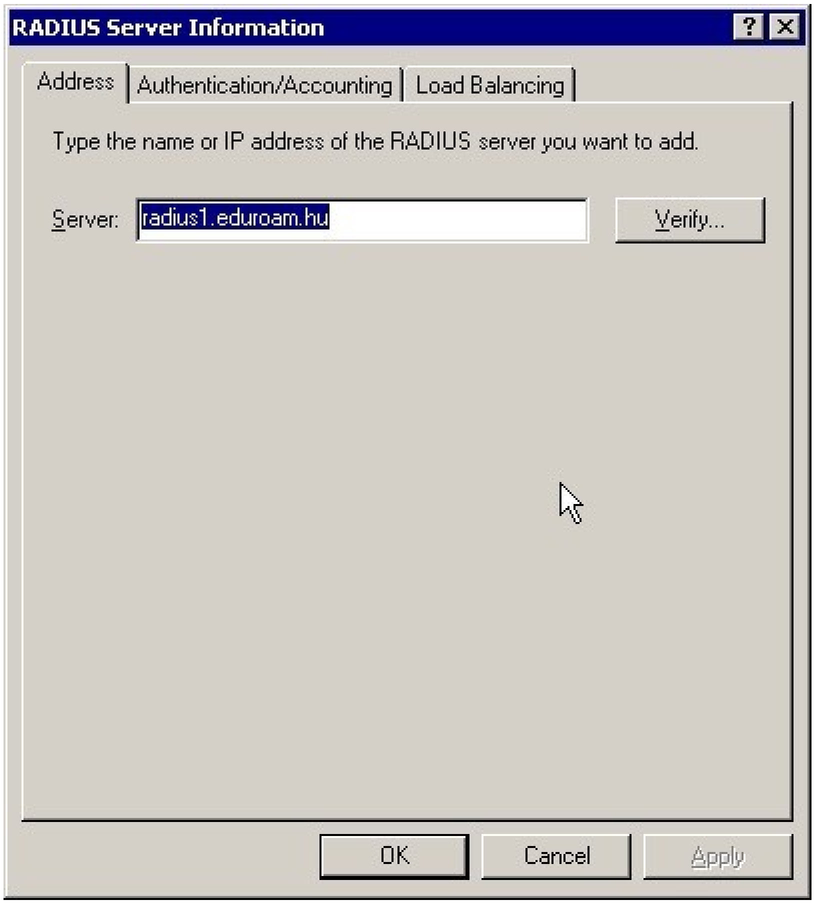


national Properties

Group name: national

RADIUS Server	Priority	Weight
radius1.eduroam.hu	1	50

The remote radius server address must be specified:

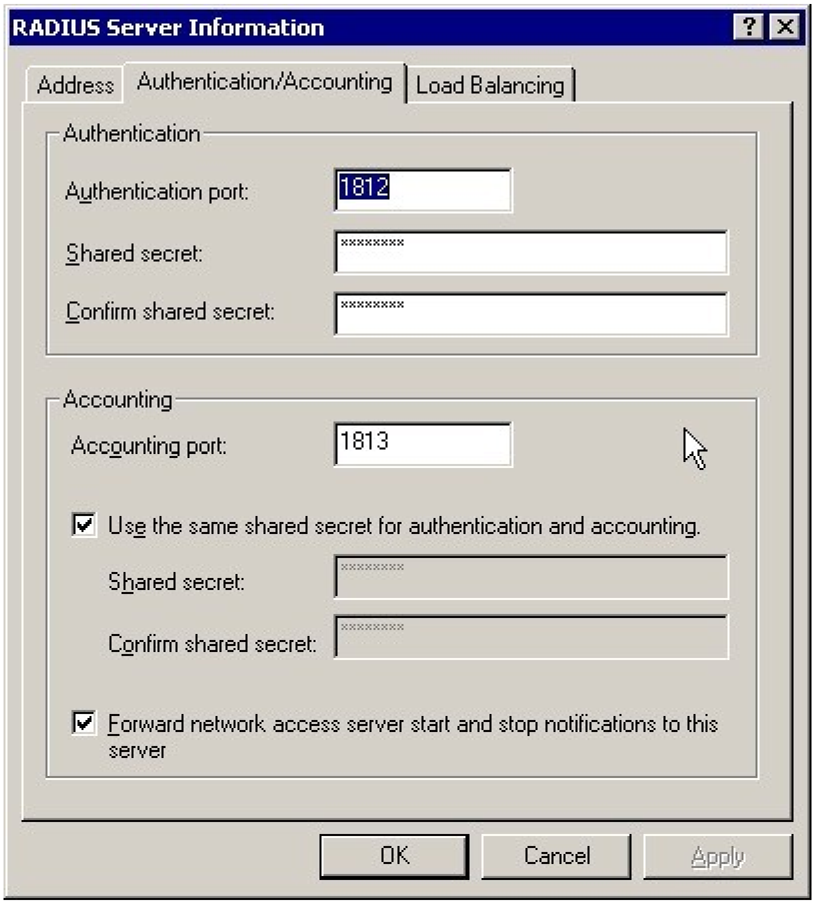


RADIUS Server Information

Type the name or IP address of the RADIUS server you want to add.

Server: radius1.eduroam.hu

with the radius server authentication port (usually 1812) and shared secret to remote radius proxy server and the remote radius server accounting port. You can specify different accounting shared secret if you wish:



Authentication

Authentication port: 1812

Shared secret: ********

Confirm shared secret: ********

Accounting

Accounting port: 1813

☑ Use the same shared secret for authentication and accounting.

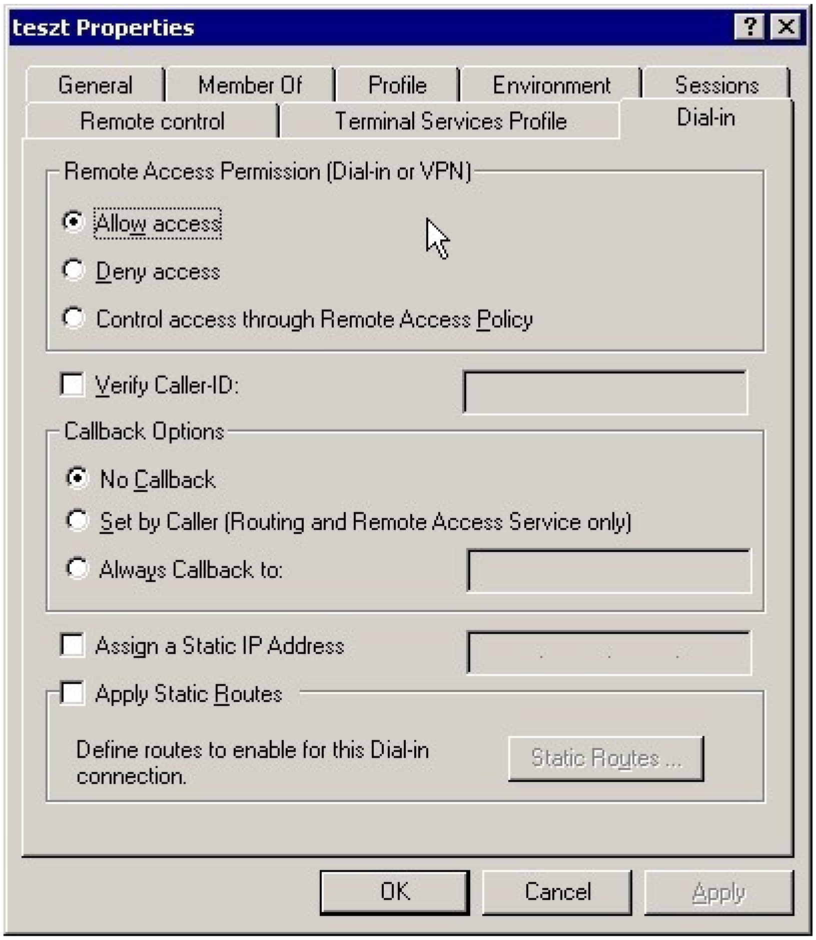
Shared secret: ********

Confirm shared secret: ********

☑ Forward network access server start and stop notifications to this server

Configuring Domain Users to be able to use the Eduroam with their credentials to Windows Domain

By default the users configured in the Windows Domain are not able to use their Windows Domain username and password to authenticate against IAS. This should be enabled in the Domain to allow access to Remote Access Permisssion. This can be done via User Management interface or Domain Manager interface with a policy:



teszt Properties

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

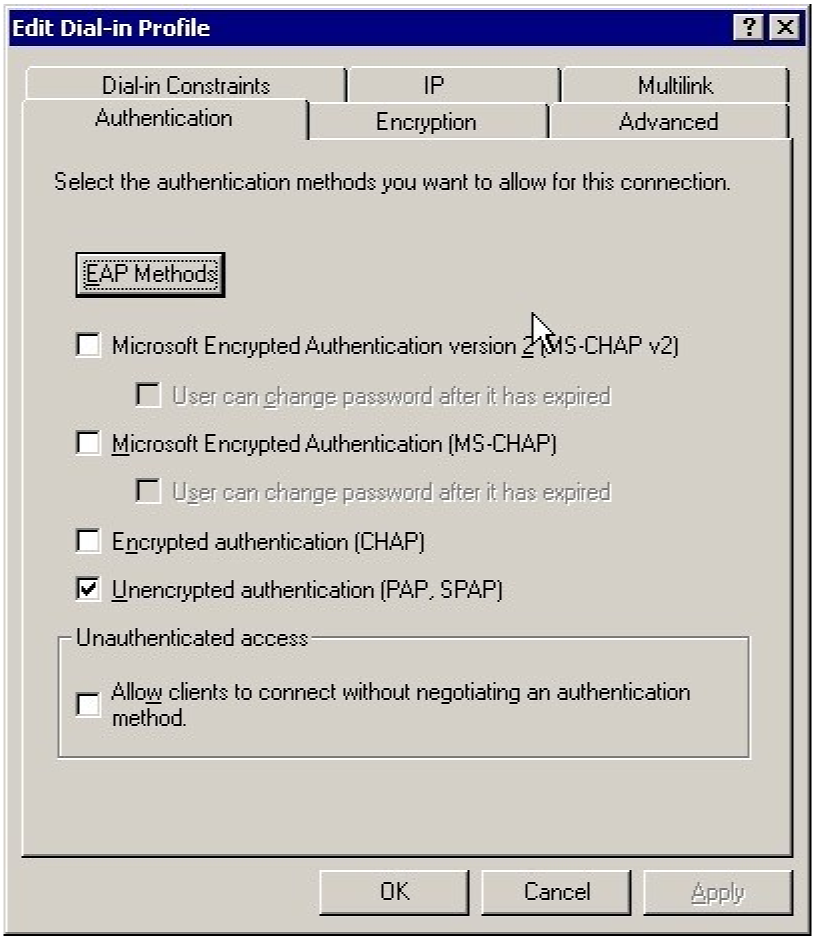
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Configuration of Authentication methods

The authentication methods should be configured in the **Remote Access Policies** under the **Profile** settings. The absolut minimum that must be enabled the PEAP under the EAP methods, but it is useful to have PAP also for debugging purpose – at least for certain accounts (e.g. For test accounts):



Select the authentication methods you want to allow for this connection.

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

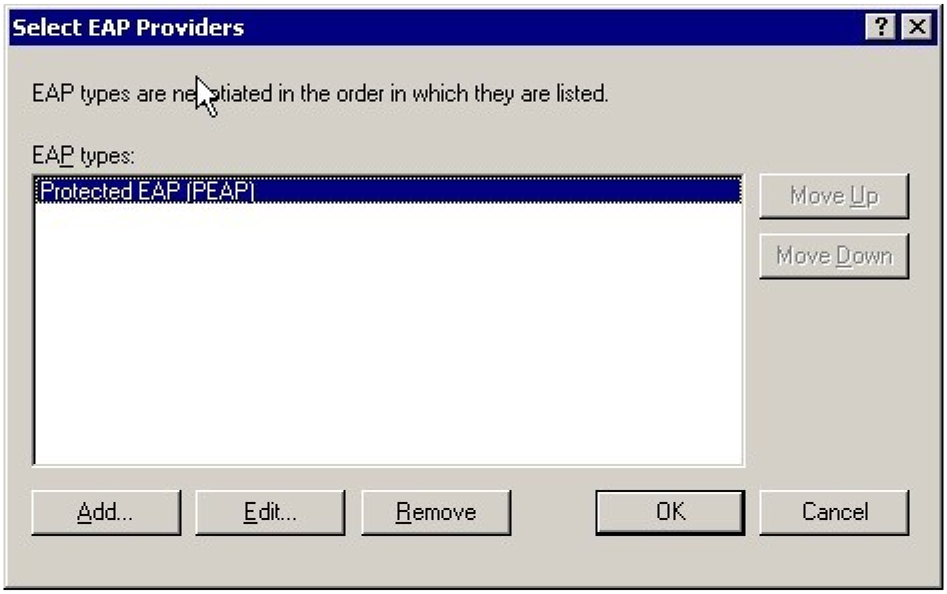
□ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

The PEAP is the easiest to deploy Eduroam authentication method under Windows. Deploying EAP-TLS can be labour-intensive:



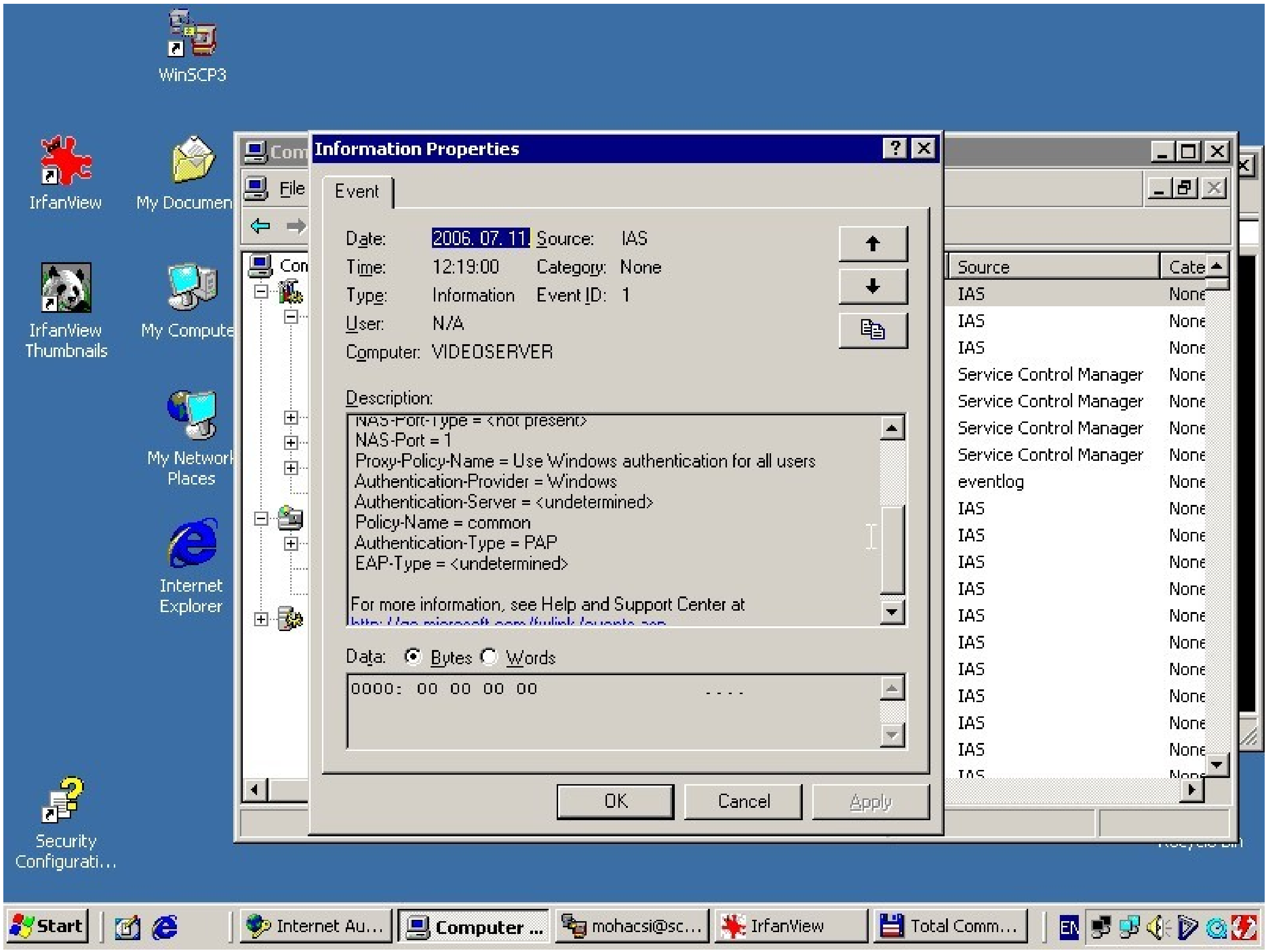
EAP types are negotiated in the order in which they are listed.

EAP types:

Protected EAP (PEAP)

Troubleshooting

The most useful information can be extracted from the Eventviewer:



Date: 2006. 07. 11. Source: IAS
Time: 12:19:00 Category: None
Type: Information Event ID: 1
User: N/A
Computer: VIDEOSERVER

Description:

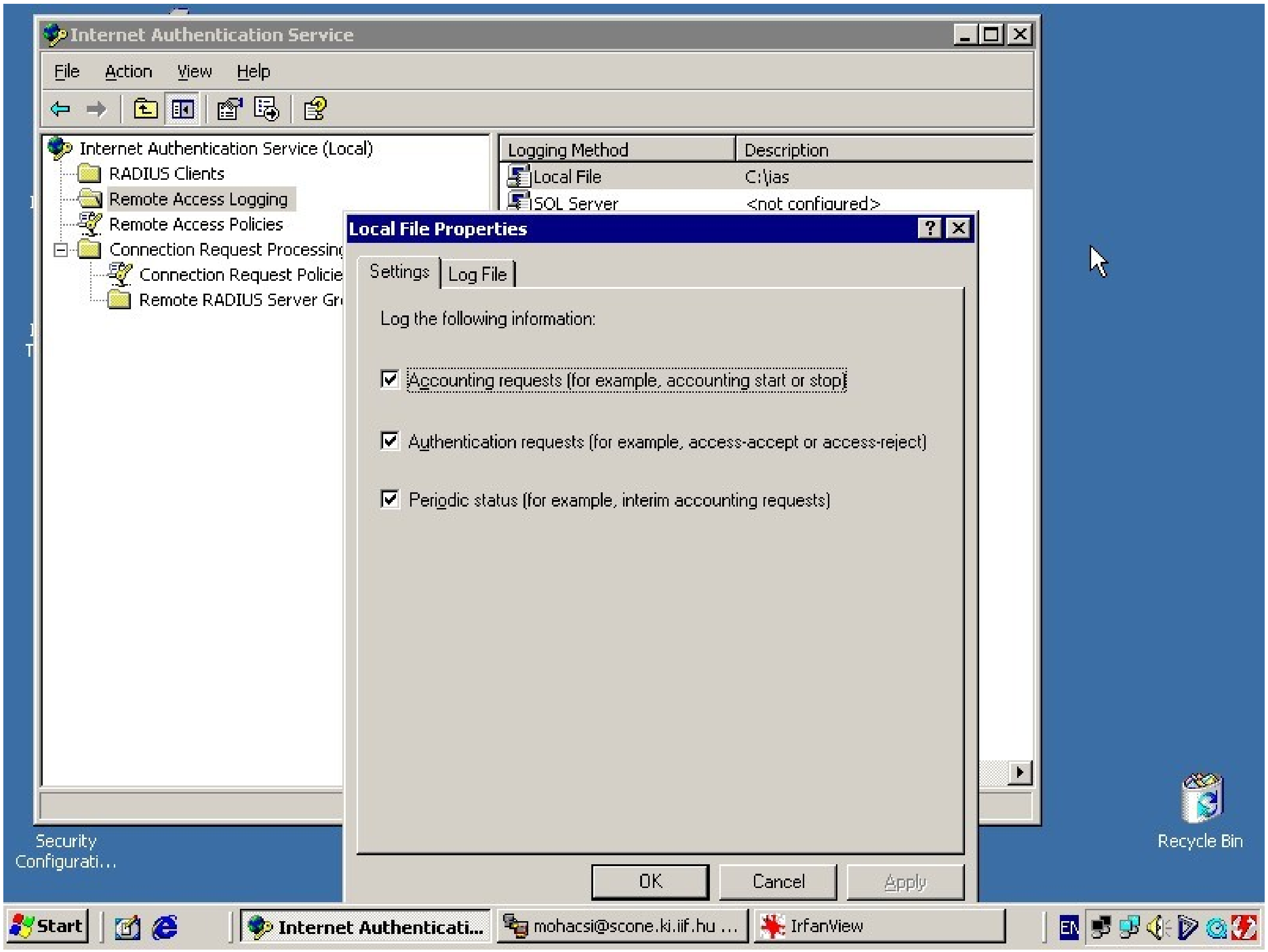
```
NAS-Port-Type = <not present>
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = common
Authentication-Type = PAP
EAP-Type = <undetermined>

For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp
```

Data: ● Bytes ○ Words

```
0000: 00 00 00 00                ....
```

Source	Cate
IAS	None
IAS	None
IAS	None
Service Control Manager	None
Service Control Manager	None
Service Control Manager	None
Service Control Manager	None
eventlog	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None
IAS	None

But you can obtain also from the log files:



Logging Method	Description
Local File	C:\ias
SQL Server	<not configured>

Local File Properties

Log the following information:

☑ Accounting requests (for example, accounting start or stop)

☑ Authentication requests (for example, access-accept or access-reject)

☑ Periodic status (for example, interim accounting requests)

References

IAS Resources: http://technet2.microsoft.com/WindowsServer/en/Library/f6985d5d-d4c5-49e2-bbc7-385e105bfe281033.mspx?mfr=true

Internet Authentication Service http://technet2.microsoft.com/WindowsServer/en/Library/d98eb914-258c-4f0b-ad04-dc4db9e4ee631033.mspx?mfr=true

IAS Pattern matching syntax: http://technet2.microsoft.com/WindowsServer/en/Library/6e5ce48d-e662-435c-a74e-0dce305914ce1033.mspx?mfr=true