TECHNICAL WHITE PAPER

Avaya G700 / G350 RADIUS Configuration Overview

Version: **1.0**

Date: **April 22, 2004**

CID: **104207**

Author: **Avaya Technology and Consulting**
Corporate Systems Engineering

Abstract:

The Internet Authentication Service (IAS) in Microsoft Windows 2000 is the Microsoft implementation of Remote Authentication Dial-in User Service (RADIUS). IAS performs centralized authentication, authorization, and accounting (AAA) of connections for dial-up and virtual private network (VPN) remote access and demand-dial connections.

This document describes how to configure IAS to authenticate switch administrators who log into the Avaya G700 and G350 media gateways, allowing RADIUS to be used as an external authentication database for switch authentication and authorization.

1. Before you begin

- The IAS is part of the Windows 2000 Server package. Make sure you have the Internet Authentication Service installed on the server.

- In the examples given in this document, IAS was installed on a Domain Controller so the Active Directory and IAS will be on the same server. It is not essential to have IAS installed on an Active Directory server, though that might be the case in large networks. IAS uses the users and groups defined on the server it is installed on, these users and groups can be defined locally on that server.

- Make sure you have TCP/IP connectivity between IAS and the G700/G350.

2. G700/G350 configuration

The G700/G350 will ask for user authentication from the RADIUS server only in case the accessing user is not defined in the locally stored internal users list. Use “show user” on the G700/G350 to view the internal users list.

Basically, the G700/G350 configuration is the same for all supported RADIUS servers. There are no special definitions required to work with IAS. Here is an example for the G350 RADIUS authentication configuration:

```
G350-002(super)# show radius authentication

Mode:                   Enable
Primary-server:         192.168.1.205
Secondary-server:       172.16.1.205
Retry-number:           4
Retry-time:             5
UDP-port:               1812
shared-secret:          *****
```

3. Users definition

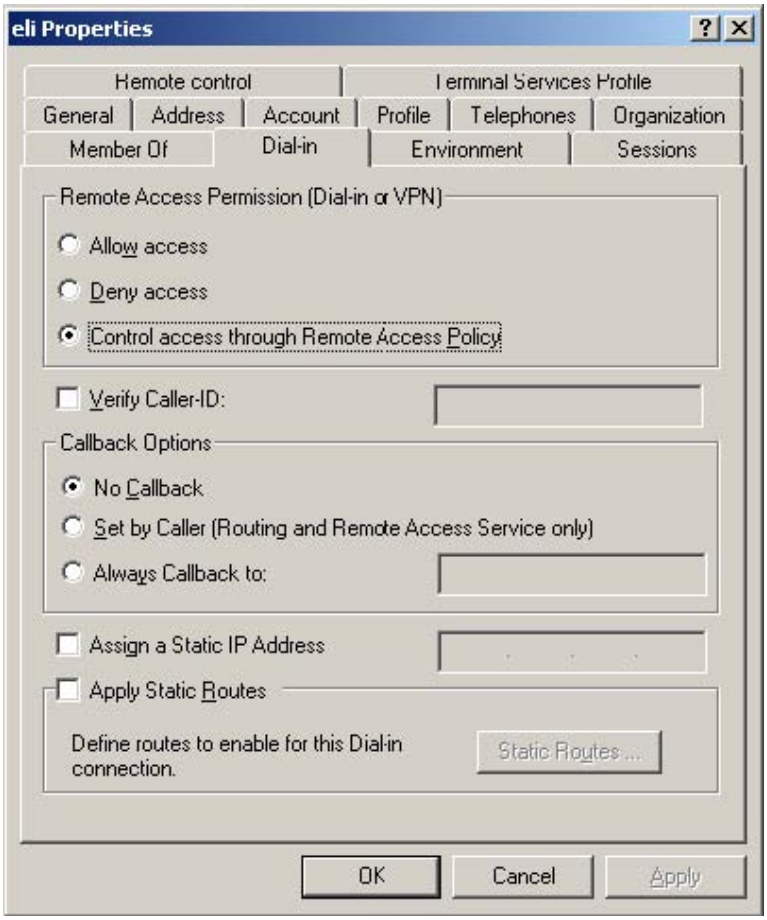
As mentioned earlier, all the user definitions are done through Active Directory. It is recommended you follow all the steps below:

- Use Start->Programs->Administrative Tools-> Active Directory Users and Computers for users and groups definition.

- First you have to define 3 user groups according to the 3 supported user levels: Read-Only, Read-Write and Admin. You can also define less than 3 grant groups, according to the access levels you wish to grant your users.

- Define the users. Follow the instructions on the screen.

- After a user is defined, go to User Properties (by clicking the right mouse button while pointing to the user). Then click on the **Dial-In** tab. Select the "Control access through Remote Policy" option in the Remote Access Permission menu.



- Click the **Member Of** tab. Add the group you want the user to belong to (Read-Only, Read-Write or Admin). Make sure you add only one of these groups.

- Click OK.

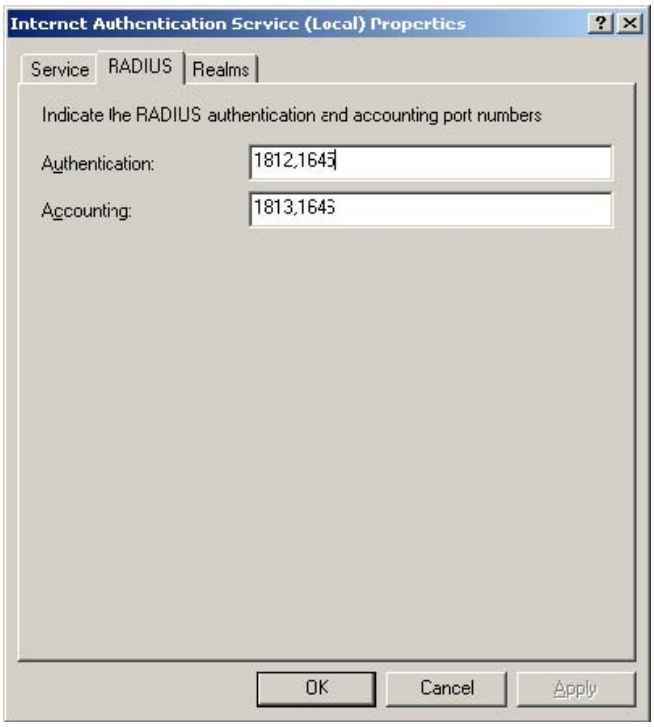
- Assign all the users to their relevant group according to the above description.

4. IAS definition

The first step will be going through the general IAS configuration:

- Open the IAS application window by clicking Start->Programs->Administrative Tools-> Internet Authentication Service

- Go to Actions->Properties. Click on the RADIUS tab. Make sure the RADIUS UDP port numbers are as follows:



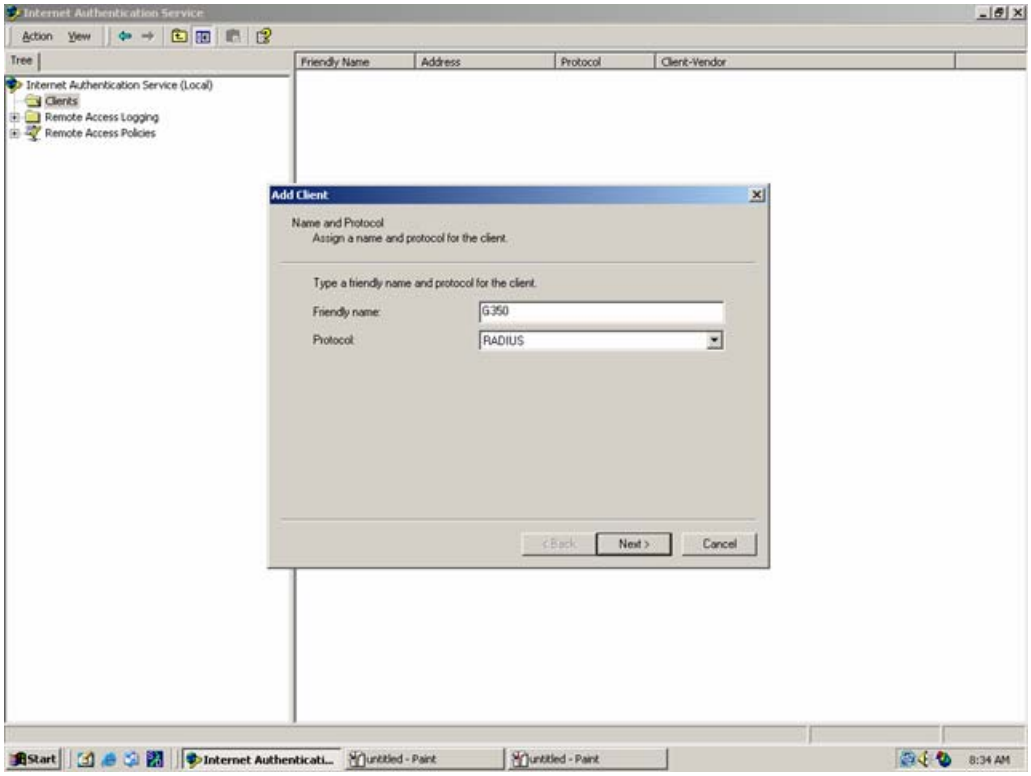
- Please note that the default port number 1812 appears in the G700/G350 RADIUS configuration. If you like, you can configure your G700/G350 to work with port 1645 instead.

- Click OK.

The second step is defining RADIUS clients:

- Double click on the **Internet Authentication Service** on the tree in the left side of the window.

- Click on **Clients** on the tree in the left side of the window. Click the right mouse button while pointing on the right side of the window. Select *New->Client.*

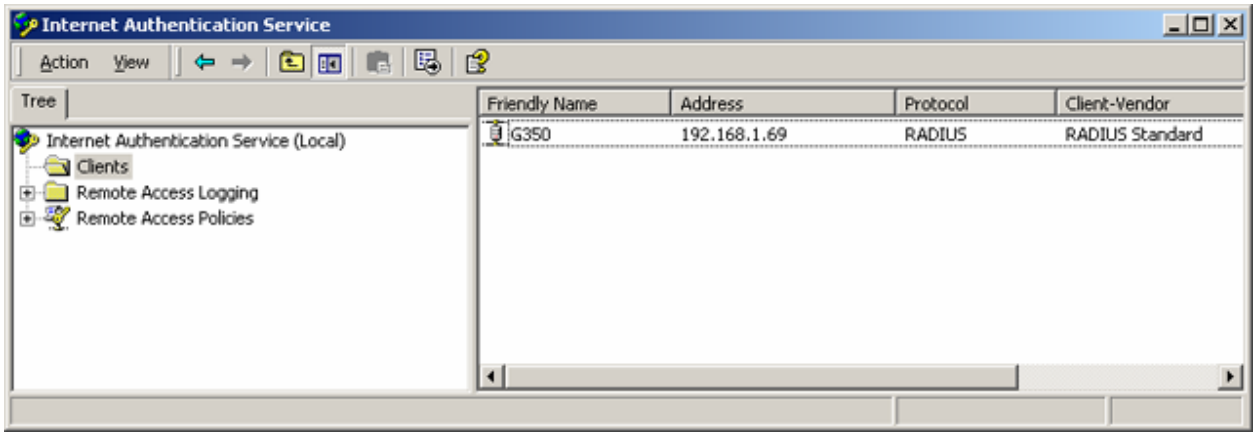


- Friendly name: G350, Protocol: RADIUS

- Click Next.

Client Address: Enter the G350 IP address. Client Vendor: RADIUS Standard Clear the “Clients must…” checkbox. Enter the shared secret according to the one defined on the G350. Confirm the shared secret by re-entering it.

- Click Finish

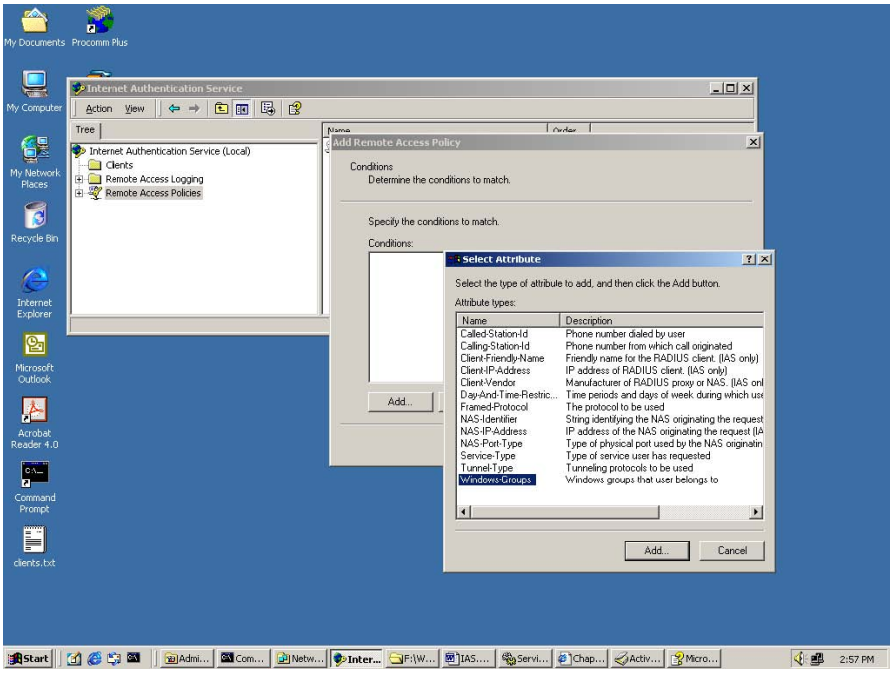


- Repeat the above steps for all the RADIUS clients you wish to use with IAS.

The next step is defining the Remote Access Policies. The IAS uses remote access policies to determine whether to accept or reject connection attempts.

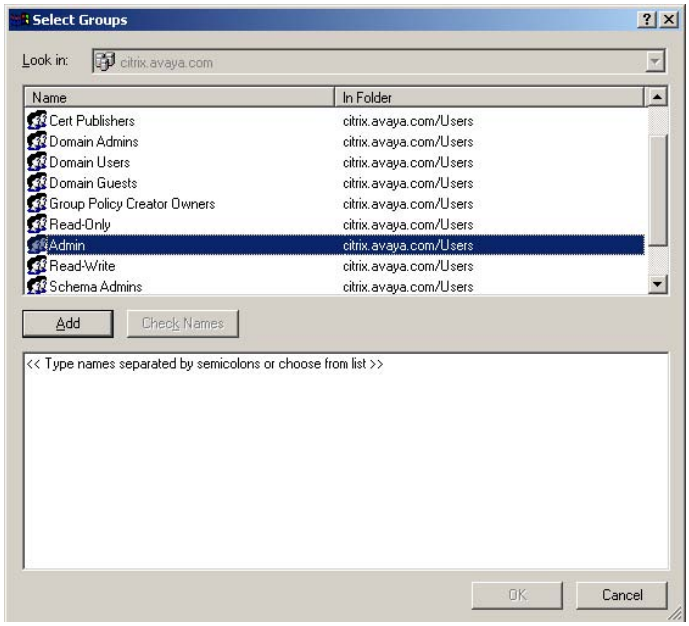
The access policies are ordered in a list (in the right side of the window) and are based on first match (a similar methodology when configuring firewall rules or access list).

- Click on the **Remote Access Policies** which on the left side of the window. Click on the right mouse button.
- Select *New Remote Access Policy.*
- The appearing dialog-box asks you to give the policy a name, then press Next.
- In the next dialog-box you should press Add.
- Select “Windows-Groups” from the list, and press Add twice.

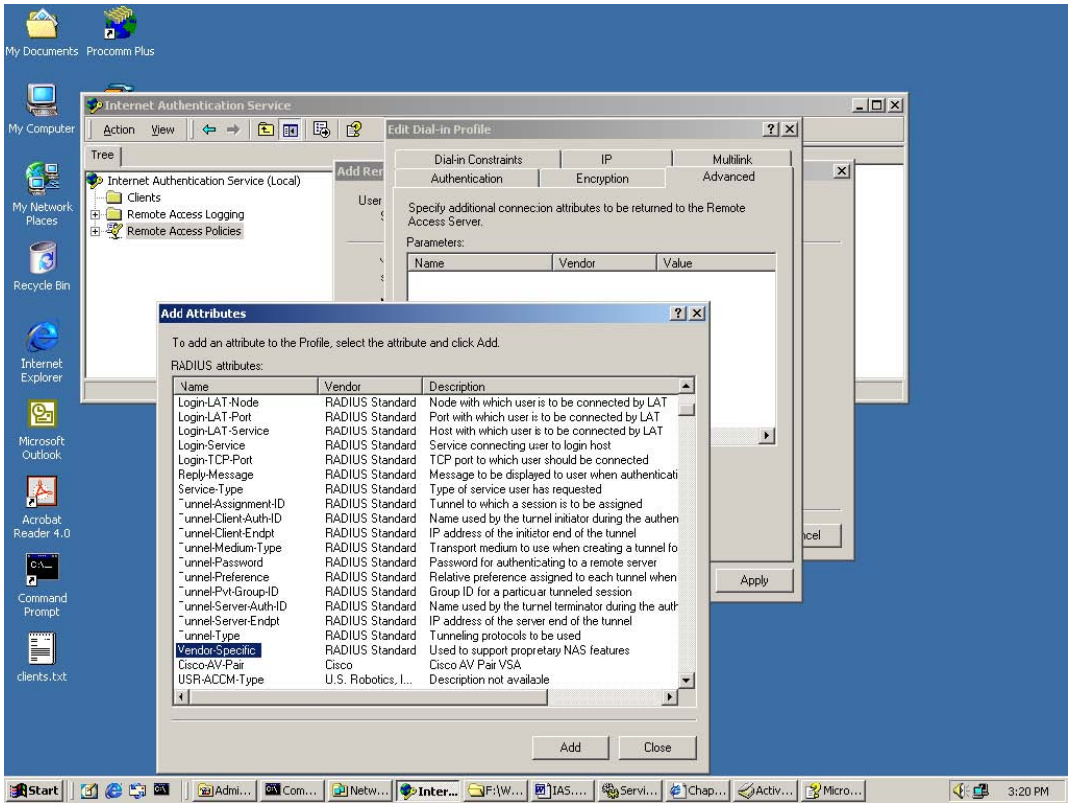


- In the following dialog-box you are asked to associate a group you've defined in the Active Directory to the specific Remote Access Policy.

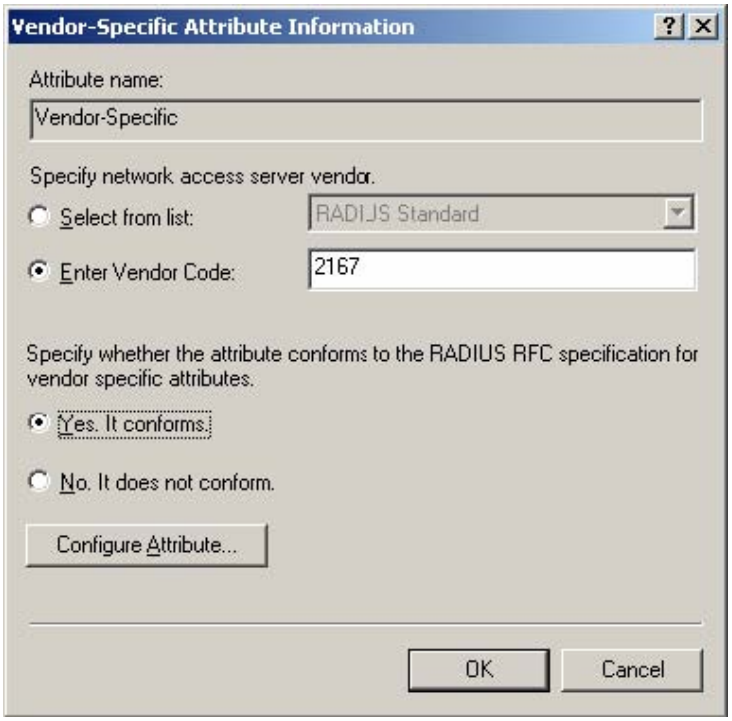
- From the groups list choose one of the groups (Read-Only, Read-Write or Admin) and press Add. Then press OK twice.



- Press Next.
- Select “Grant remote access permission”, then press Next.
- Press Edit Profile.
- In the appearing dialog-box go to the **Authentication** tab. Clear the checkboxes of MS-CHAP and MS-CHAP v2. Mark the checkboxes of CHAP and PAP, SPAP. Press Apply.
- Go to the **Advanced** tab. Remove all the items from the list so it is empty.
- Press Add.



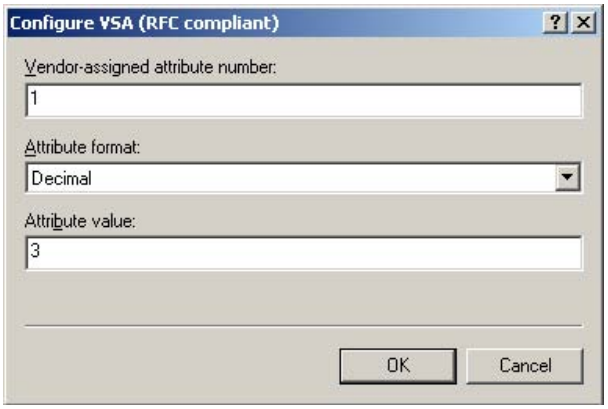
- Select “Vendor-Specific” from the list, and press Add twice.
- Select “Enter Vendor Code”. Type 2167 in the vendor field.



- Select “Yes, It conforms”. Press Configure Attribute.

- In the following dialog box fill in the following parameters: Vendor-assigned attribute number: 1

- Attribute format: Choose “Decimal” from the list.
    - Attribute Value: Should be set according to the group grant: Read-Only: 1 Read-Write: 2 Admin: 3



Press OK three times.

- Close the dialog box. Then press OK and Finish.

- Repeat the above steps in order to define Remote Access Policies for all the 3 groups. Each grant group should have at least one Remote Access Policy entry.

The last step is to register the IAS in Active Directory:

- Select *Internet Authentication Service* on the left side of the application window.

- Click on the right mouse button. Select **Register Service in Active Directory**.

5. Troubleshooting

- Make sure the IAS service is up and running. You can use *Start->Programs->Administrative Tools->Services* to view the status of the service.

- Use *Start->Programs->Administrative Tools->Event Viewer* to view the logs.

- View the IAS specific log activity which defaults in the directory (drive:\WINNT\system32\Logfiles).

END