

Remote Access Technical Guide To Setting up RADIUS

V 2.4
Published: 09 May 2006



1 Index

1 Index.....	2
1.1 Other Relevant Documents	2
2 Introduction	3
2.1 Authentication realms	3
2.2 Installing IAS	4
2.3 Configuring IAS	4
2.3.1 IAS Properties.....	4
2.3.2 RADIUS Clients	4
2.3.3 Remote Access Logging	4
2.3.4 Remote Access Policies	5
2.3.5 Connection Request Policies	5
2.3.6 Inform CLEO About Your RADIUS Server	6
2.4 Managing Users, Groups and Services	6
2.5 Configuring ISA Server.....	7

1.1 Other Relevant Documents

The following list includes all documents and forms required for the CLEO remote access services. Please ensure you have read all documents relevant to the service you require:

Documents relevant to all services:

- Introduction to CLEO Remote Access Services – A Short Guide for Headteachers and Senior Managers
- Introduction to CLEO Remote Access Services – A Detailed Guide to the Benefits and Risks, for Headteachers and Senior Managers
- Best Practice Guide to Preparing Your School Network and Remote Users PCs
- CLEO Remote Access Services Terms & Conditions, and Acceptable Use Policy
- Initial Enquiry Form

Documents specific to individual services:

- Technical Guide – Setting up CLEO Web Gateway
- Technical Guide – Setting up CLEO VPN
- Technical Guide – Setting Up RADIUS
- Technical Details Submission Form – available online for each service

2 Introduction

This technical guide describes how to set up RADIUS on your school server to enable remote users to be authenticated before accessing resources and files stored on the server. **RADIUS** needs to be set up for the following CLEO remote access services:

- **Authentication for the VPN solution**

The structure of the distributed RADIUS service is relatively straight forward, each institution maintains a RADIUS service running on one or two of their servers, normally the domain controllers (DC), running Microsoft Internet Authentication Service (IAS). IAS is included with the all versions of the Windows 2003 Server licence (except web server). The additional load on the DC is minimal and the security risk is considered low.

If your institution runs a MS ISA server, then install IAS on this server instead. There are other steps specific to institutions running ISA server, see appendix A - ISA Server.

In the core CLEO maintains a number of RADIUS proxy servers; these determine which institution a user originates from and forwards the authentication request accordingly.

2.1 Authentication realms

For the proxy servers in the CLEO core to be able to forward requests appropriately users provide an authentication realm, this takes the following form:

<username>@<authentication-realm>

temp@office.cleo.net.uk

To ensure uniqueness in the naming of authentication realms we are going to use:

Lancashire Schools:	.lancs.sch.uk
Cumbrian Schools:	.cumbria.sch.uk
CLEO office, etc...	.cleo.net.uk

This realm need not match your windows 2003 domain and the method to translate from one to the other is explained in the **configuring IAS** section of this guide.

Microsoft Internet Authentication Service (IAS) is the Microsoft RADIUS service and is freely available as part of the Windows 2003 Server License (except web server edition).

2.2 Installing IAS

1. **Control Panel, Add or Remove Programs, Add/Remove Windows Components.**
2. In the **Windows Components Wizard**, highlight **Network Services** in Components list and click **Details...**
3. In the **Networking Services** dialog check **Internet Authentication Service** and click **OK**.
4. In the **Windows Components Wizard**, click **Next** and **Finish**.

2.3 Configuring IAS

Go to All Programs\Administrative Tools\Internet Authentication Service

2.3.1 IAS Properties

1. Right click on the **Internet Authentication Service (Local)** snap-in and select **Properties**.
2. **On the General** tab, check Rejected Authentication Requests & Successful authentication requests.
3. **Ports** tab, confirm that **Authentication** contains *1812 only*, and that **Accounting** contains *1813 only*.
4. Click **OK**.

2.3.2 RADIUS Clients

The three CLEO RADIUS proxies used for the remote access service are configured within IAS as RADIUS clients. Under the Internet Authentication Service (IAS) snap-in within your MMC, right click on the **RADIUS Clients** folder and select **new Radius Client** from the pop-up menu. In the **New RADIUS Client** dialog enter the following details:

Friendly name:	Client Address (IP or DNS)	Client-Vendor	Shared secret/ Confirm shared secret
CLEO Radius Proxy 0	AAA0.cleo.net.uk	RADIUS	a complex password See note
CLEO Radius Proxy 1	AAA1.cleo.net.uk	RADIUS	
CLEO Radius Proxy 2	AAA2.cleo.net.uk	RADIUS	

Note:

This secret should be a complex password (see Microsoft's guidance notes on complex passwords or enter "complex passwords" in search on www.microsoft.com for more info).

2.3.3 Remote Access Logging

These settings allow you to configure how, what and where the remote access logs are generated:

1. Open Remote Access Logging
2. Right click on Local File and select **Properties**.

3. On the **Settings** tab, it is recommend that the following are selected **Accounting requests** and **Authentication requests**. The **Periodic status** one is not required.
4. On the **Log File** tab use the **Browse** button to locate a directory on a data drive in which to store the log files. Under **Format** select **Database-compatible**, and under **Create a new log file:** selected **Daily**.

2.3.4 Remote Access Policies

Using the **Active Directory Users and Computers** create a Global group called 'VPN Administrator Access Group' and make any technicians and administrators that you want to have VPN access members of this group.

Note: For every user that you add to the group, you must also enable Dial-In or VPN access. Right click on the user that you have added to the group, and click properties. Click on the "Dial-In" tab, and under "Remote Access Permission, click "Allow Access". Click on "OK" to apply the change.

1. In the **Internet Authentication Service**, left click on the **Remote Access Policies** folder and delete any default policies.
2. Right click on the **Remote Access Policies** folder and select **New Remote Access Policy**.
3. Click **Next**, select **Use the wizard to set up a typical policy for a common scenario**, in the **Policy name:** box enter 'Administrator Access' and click **Next**.
4. Select **VPN** and click **Next**.
5. Select **Group** and click **Add**. In the **Select Groups dialog** type 'VPN Administrator Access Group' and click **OK**.
6. On the **New Remote Access Policy Wizard**, click **Next**.
7. On the **Authentication Methods** page check that **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** is selected and click **Next**.
8. On the **Policy Encryption Level** page ensure all three encryption options are selected and click **Next**.
9. Click **Finish**.

2.3.5 Connection Request Policies

Only one policy is normally necessary for this option, by default it is named **Use Windows authentication for all users**.

1. Open Internet Authentication Service & double click Connection Request Processing
2. **Click on Connection Request Policies**
3. **Right click Use Windows authentication for all users**
4. Click Properties
5. Now click **Edit Profile**, edit the settings:
6. **Authentication** tab: **Authenticate requests on this server** should be selected.

7. **Accounting** tab: nothing to set.
8. **Attribute** tab: In the drop down list named Attribute select User-Name. Click **Add**. In the **Find** box type the @<school>.<LEA>.sch.uk assigned as the RADIUS realm and in the **Replace With** box type the Windows Active Directory domain name. e.g. @caldew.cumbria.sch.uk and @caldew.local
9. **Click OK**
10. **Advanced** tab: nothing to set. Click OK
11. **Click OK**

2.3.6 Inform CLEO About Your RADIUS Server

Once you have configured your site RADIUS server please email [your](#) LA support with the following details:

Server type: [MS-IAS, FreeRADIUS, etc...]

Server IP: [10.x.y.z]

Server Secret: [strong password]

RADIUS Realm: [.sch.uk domain name]

If you have IP based Network or server security in place add a rule to

Allow UDP 1812,1813 10.64.134.0/24 inbound & outbound

For remote access clients to be able to access services and resources on your network you will need to configure your network and server firewalls to trust the remote access network IP address range provided for your site. The level of trust that you give to this subnet is entirely up your institution, but it is worth bearing in mind that restricting access to certain services such as local DNS, Kerberos, LDAP, WINS, etc may create problems for clients connecting remotely.

2.4 Managing Users, Groups and Services

Careful consideration should be made of how to implement VPN access. CLEO recommends that VPN access is only made available to Technical and certain key teaching staff. Future CLEO services will enable staff & pupils a more robust solution.

For ease of support both within individual institutions and within the LA's as a whole it is recommended that access is provided in a staged fashion. This sort of rollout should allow any issues to be resolved with end users, who have the motivation and experience to work through them with those providing technical support.

All CLEO remote access services are provided subject to the terms and conditions described in the “**CLEO REMOTE ACCESS SERVICE ACCEPTABLE USE POLICY**”. Please ensure you have read, understand and abide by the conditions described.

All services are renewable on an annual basis and CLEO reserves the right to withdraw, suspend or modify all elements of the service at any time.

BE RESPONSIBLE – BE SECURE AND ENJOY WORKING FLEXIBLY!

2.5 Configuring ISA Server

Where a schools IAS server and resource that are to be accessed remotely are protected by an ISA server then some additional configuration needs to be done. The instructions below detail how to configure IP Filters and Server Publishing settings for your RADIUS server.

Using the **ISA** MMC snap-in, go to **Servers and Arrays**, <my ISA server>, **Access Policy**, **IP Filters**.

1. Click **Create a Packet Filter**,
2. In the **new IP Packet Filter wizard** dialog, in **IP packet filter name** enter *RADIUS Auth* and click **Next**.
3. Select **Allow packet transmission**, and click **Next**.
4. Select **Custom** and click **Next**.
5. On the **Filter settings** page,
 - i. **IP Protocol**, *UDP*
 - ii. **Direction**, *Both*
 - iii. **Local Port**, *1812*
 - iv. **Remote Port**, *All Ports*
 - v. Click **Next**.
6. Select **Default IP address for each external interface on the ISA server computer** and click **Next**.
7. Select **All Remote Computers** and click **Next**.
8. Click **Finish**.
9. Select *RADIUS Auth* from the list of filters and click **Configure a Packet Filter**.
10. On the **Remote Computer** tab, select **This range of computers:** and enter **Subnet** *10.64.134.0*, **Mask** *255.255.255.0* and click **OK**.
11. Repeat steps 1 to 10 but name the filter *RADIUS Acc* and specify **Local Port** *1813*.

Now go to **Policy Elements**, **Protocol Definitions**.

12. Click **Create a Protocol Definition**,

13. In the **new protocol definition** dialog, in **Protocol definition name** enter *RADIUS Auth/Acc* and click **Next**.
14. **Port number** *1812*, **Protocol type** *UDP*, **Direction** *Receive Send* and click **Next**.
15. Click **Yes**, click **New**.
16. Port range **From** *1812*, **To** *1813*, **Protocol type** *UDP*, **Direction** *Receive Send*, click **OK**.
17. Repeat '5' but with **Direction** *Send Receive*.
18. Click **Next**.
19. Click **Finish**.

Now go to **Server Publishing Rules**.

20. Click on **Publish a Server**.
21. In the **New Server Publishing Rule Wizard**, **Server Publishing Rule Name**, enter *RADIUS Server* and click **Next**.
22. In **IP address of internal server** enter the IP address of the server running **IAS** (e.g. 192.168.x.y) and in **External address on ISA server** browse to the external IP address of this ISA server (e.g. 10.x.y.z) and click **Next**.
23. In the **Apply rule to this protocol:** combo select *RADIUS Auth/Acc* and click **Next**.
24. Select **Specific computers (client address sets)** and click **Next**.
25. Under **client address sets**, click **Add**.
26. On the **client address sets** dialog click **New**.
27. On the **client set** dialog enter:
 - i. **Name** *CLEO AAA Servers*
 - ii. **Description** *<optional>*
 - iii. **Members** click **Add**, **From** *10.64.134.2 To 10.64.134.254*.
28. Check that *CLEO AAA Servers* is listed in **include these sets** and click **OK**.
29. Click **Next**.
30. Click **Finish**.

You will also need to configure IP Filters, and publish any local server resource you wish to make available to your remote users (see **Ancillary Services** section for the basic services).

The details of the remote access subnet for your site will be provided to you in the confirmation email when you inform CLEO about the settings for your RADIUS (MS-IAS) server.