Errata
E2000 Manual 1.3.0

This document provides information on how to configure Radius and Tacacs+ authentication in the E2000, which will be included in future releases of the E2000 Manual.

Order of Topics:

How to configure Radius in E2000

There are two ways to set the authentication method in E2000:

- During the Initial Setup (through the wizard in the first boot)
- By typing the command "setauth" in the shell of the E2000

While configuring Radius authentication, the system will prompt you for the IP address of the RADIUS server and the secret (configured in the server).

After setting the authentication method in E2000, add the user in the database of the E2000 to enable the system to remotely authenticate and authorize user access.

To execute this step:

1. From the E2000 web interface, log in as **admin**.

2. Add the user to be authenticated remotely by selecting the **User** tab and filling in the form.

The default ports that are used for Radius Authentication are:

- 1812: for Radius authentication
- 1813: for Rdius accounting

Configuring Radius during the Initial Setup

When you select Radius as the authentication method, the system prompts you for other Radius servers to be configured, thus allowing you to configure more than one Radius Server.

Example:

```
Welcome to Cyclades-APM!
Since this is the first time you are booting your APM, you need to
answer some basic configuration questions. Once this is done, the
other APM configuration parameters can be set through its Web
Management Interface (WMI).
Press any key to continue.
You must now set a password for 'root', the system administrative
account.
WARNING: This is a very powerful account, and as such it's advisable
that the password is chosen with care and kept within the reach of
system administrators only.
New password:
Re-enter new password:
Password changed
You must now set a password for 'admin', the administrative account
for the Web Management Interface (WMI).
WARNING: this is a very powerful account, and as such it's advisable
that the password is chosen with care and kept within the reach of
system administrators only.

New password:
Re-enter new password:
Password changed
Please choose the time zone where this machine is located.
1) Africa     18) Eire      35) Jamaica     52) ROC
2) America    19) Etc       36) Japan       53) ROK
3) Antarctica 20) Europe    37) Kwajalein   54) Singapore
4) Arctic     21) Factory   38) Libya       55) SystemV
```

```
5) Asia         22) GB          39) MET         56) Turkey
6) Atlantic     23) GB-Eire     40) MST         57) UCT
7) Australia    24) GMT         41) MST7MDT     58) US
8) Brazil       25) GMT+0       42) Mexico      59) UTC
9) CET          26) GMT-0       43) Mideast     60) Universal
10) CST6CDT     27) GMT0        44) NZ          61) W-SU
11) Canada      28) Greenwich   45) NZ-CHAT     62) WET
12) Chile       29) HST         46) Navajo      63) Zulu
13) Cuba        30) Hongkong    47) PRC         64) iso3166.tab
14) EET         31) Iceland     48) PST8PDT     65) posix
15) EST         32) Indian      49) Pacific     66) posixrules
16) EST5EDT     33) Iran        50) Poland      67) right
17) Egypt       34) Israel      51) Portugal    68) zone.tab

Enter the number corresponding to your choice: 8
1) Brazil/Acre 3) Brazil/East 5) Back
2) Brazil/DeNoronha 4) Brazil/West
Enter the number corresponding to your choice: 3
Current system date and time is:
    Thu Apr 21 09:58:43 BRT 2005
Press ENTER to accept it or specify new ones.
Enter date in MM/DD/YYYY format: 04/20/2005
Enter time in HH:MM format: 10:00
Wed Apr 20 10:00:00 BRT 2005

Primary Ethernet IP address: (S)tatic or (N)one ? [S]:
Enter Primary Ethernet IP address: 192.168.110.10
Enter Primary Ethernet Subnet Mask: 255.255.0.0
Secondary Ethernet IP address: (S)tatic or (N)one ? [S]: N
Configure Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]:
Configure Ethernet VLANs: (Y)es, (N)o or (L)ist ? [N]:
Enter Ethernet Default Gateway [none]: 172.20.0.1
Enter the System's Hostname
    (max 30 characters) [E2000]:
Enter the System's Domain Name
    (max 60 chars) [localdomain]:
Enter the Primary Nameserver's IP address [none]:
Enter the NTP server:
Enter the email (SMTP) server:
Choose the desirable authentication method
    (local/radius/tacacs+/ldap/kerberos/nis/active_directory)
[local]: radius
Enter the radius server: 192.120.0.3
```

```
Supply the secret for this radius server:
Confirm the shared secret:
Configure another radius server? (y/n)[n]: y
Enter the radius server: 172.20.105.36
Supply the secret for this radius server:
Confirm the shared secret:
Configure another radius server? (y/n)[n]: n
Does the RADIUS server employ RSA SecurID authentication? (y/n)[n]:
```

Configuring Radius through the Shell comand

The command /sbin/setauth enables you to manually and individually configure specific E2000 settings through the Shell:

```
[root@E2000 root]# setauth
Your configuration will be overwritten by the default files!!
Are you sure you want to continue? (y/n)[n] y
Continuing setauth...
Choose the desirable authentication method
   (local/radius/tacacs+/ldap/kerberos/nis/active_directory) [local]:
radius
Enter the radius server: 170.120.105.30
Supply the secret for this radius server:
Confirm the shared secret:
Configure another radius server? (y/n)[n]: y
Enter the radius server: 170.120.10.2
Supply the secret for this radius server:
Confirm the shared secret:
Configure another radius server? (y/n)[n]: n
Does the RADIUS server employ RSA SecurID authentication? (y/n)[n]:

*** Configuration changed!
*** Execute saveconf to save the new values in flash.
```

After executing the command **setauth**, execute the command **saveconf** to save the changes to flash, and enable the system to use the configuration in the next boot.

Files configured in the E2000

The following files are configured with Radius Authentication:

- /etc/pam.conf
- /etc/raddb/server

Enabling the Radius user in the E2000

Any user who will use the E2000 application must be entered in the E2000 database in order to have access to the application, regardless of whether you are using any other authentication services or not. RADIUS users, for example, must still be registered in the E2000 database through the User Detail form:

1. Login into the E2000 web interface as admin user.
2. Select the tab **Users** and add the user that is created in your Radius Server.
3. If you are using another server authentication, it is not advisable that you activate the password for local authentication (checking the checkbox "Local Password").

Additional Information About Radius Server Configuration

The following files must be configured in the Radius Server:

/etc/raddb/clients : This file contains a list of clients which are allowed to make authentication requests and their encryption key. You must, for example, configure the IP Address of the E2000 and the secret that will be prompted during the setup of the E2000.

# Client Name	Key
#----------	----------
<IP_address E2000>	<secret>

/etc/raddb/naslist : This file contains a list of NASes (Network Access Servers, also known as terminal servers). The fields to be configured in this file are:

Valid hostname or the IP address of the E2000

Shortname of the file that will log accounting.

This means: /var/log/radacct/<shortname>/detail

Third field defines what type of device it is.

For example:

NAS Name Short Name Type
#---------------- ---------- ----
<IP_address E2000> <shortname> portslave

/etc/raddb/users : This file contains security and configuration information for each user. The first field is the user's name and can be up to 31 characters in length. This is followed (on the same line) with the list of authentication requirements for that user. This can include password, comm server name,comm server port number, protocol type (perhaps set by the "hints" file), and huntgroup name (set by the "huntgroups" file).

Authentication Accounting in the Radius Server

We can verify the accounting of each authentication in the Radius Server through the following file:

tail -f /var/log/radacct/default/detail

Fri Apr 22 10:58:03 2005

User-Name = "willians"
NAS-IP-Address = 170.120.10.1
NAS-Identifier = "java_auth"
NAS-Port = 925
NAS-Port-Type = Virtual
Acct-Status-Type = Start
Acct-Session-Id = "00000925"
Acct-Authentic = RADIUS
Client-IP-Address = 170.120.108.1
Timestamp = 1114178283
Request-Authenticator = Verified

Fri Apr 22 11:09:58 2005

User-Name = "willians"
NAS-IP-Address = 170.120.10.1
NAS-Identifier = "java_auth"
NAS-Port = 918
NAS-Port-Type = Virtual

Acct-Status-Type = Stop
Acct-Session-Id = "00000918"
Acct-Authentic = RADIUS
Acct-Session-Time = 1114006165
Client-IP-Address = 170.120.10.1
Timestamp = 1114178998
Request-Authenticator = Verified

How to Configure TACACS+ in the E2000

There are two ways to set the authentication method in E2000:

- During the Initial Setup (through the wizard in the first boot)
- By typing the command "setauth" in the shell of the E2000

In the version 1.3.0 we can't configure, through the ways above, more than one server for Tacacs+ authentication. But you can configure the file /etc/pam.conf to enable the E2000 to be authenticated through more than one server.

After set the authentication method in E2000 we need add the user in the database of the E2000 to enable it to be remotely authenticated and be authorized for the system.

To execute this step:

1. From the E2000 web interface, log in as admin.
2. Add the user to be authenticated remotely selecting the tab "User" and filling the form.

The default port that is used for Tacacs+ authentication is 49.

Configuring Tacacs+ during the Initial Setup

Example:

```
Choose the desirable authentication method
(local/radius/tacacs+/ldap/kerberos/nis/
active_directory) [local]: tacacs+
Enter the TACACS+ server: 172.20.105.36
Enter the shared secret:
Confirm the shared secret:
Enter the available service [system]:
```

```
Does the TACACS+ server employ RSA SecurID
authentication? (y/n)[n] n
```

Configuring Tacacs+ through the Shell comand

The command **/sbin/setauth** enables you to manually and individually configure specific E2000 settings through the Shell:

```
[root@E2000 root]# setauth
Your configuration will be overwritten by the default
files!!
Are you sure you want to continue? (y/n)[n] y
Continuing setauth...

Choose the desirable authentication method
(local/radius/tacacs+/ldap/kerberos/nis/active_directory)
[local]: tacacs+
Enter the TACACS+ server: 170.120.100.30
Enter the shared secret:
Confirm the shared secret:
Enter the available service [system]:

Does the TACACS+ server employ RSA SecurID
authentication? (y/n)[n]:

*** Configuration changed!
*** Execute saveconf to save the new values in flash.
```

After executing the command **setauth**, execute the command **saveconf** to save the changes in the flash, and enable the configuration to be used in the next boot of the E2000.

Enabling the Tacacs+ user in the E2000

Any user who will use the E2000 application must be entered in the E2000 database in order to have access to the application, regardless of whether you are using any other authentication services or not. Tacacs+ users, for example, must still be registered in the E2000 database through the User Detail form as follows:

1. Login in the WebUI as admin user
2. Select the tab Users and add the user that is created in your Tacacs+ Server

3. If you are using another server authentication, it is not advisable that you activate the password for local authentication (checking the checkbox "Local Password").