

Configuring SafeWord® PremierAccess™ for Interoperability with Check Point™ Connectra™

3/17/05 A

1 Introduction

SafeWord® PremierAccess™ improves the security of applications and services protected by Connectra™ by providing Connectra with a flexible and easy to manage system for strong user authentication.

Strong user authentication is achieved by requiring users to authenticate with token-generated, one-time passwords, which avoid the vulnerabilities inherent with fixed passwords, such as password sniffing, theft and guessing. One time passwords, called passcodes are immune to these threats. Once used, a passcode is immediately invalidated by SafeWord and cannot be reused. Generated by using cryptographic algorithms, passcodes are practically impossible to guess. In addition, the tokens that generate passcodes can be PIN protected, providing strong, two-factor authentication based on something the user knows (a PIN) and something the user has (a token).

Connectra follows a specific sequence in determining the method to be used for authenticating each user. If the user has a certificate, Connectra authenticates the user via the certificate. If the user does not have a certificate, Connectra first searches its internal database for the username. If the username is found, Connectra performs the authentication. If the username is not found, Connectra searches its external databases, starting with LDAP, followed by RADIUS.

Consequently, Connectra does not have entries in its internal database for users that are identified in LDAP or RADIUS databases. When SafeWord PremierAccess is designated as the RADIUS server, PremierAccess manages usernames and their associated credentials in its own database. In Connectra all of these users are represented by the generic username *generic**. Upon a successful authentication PremierAccess returns to Connectra a RADIUS attribute containing the names of the RADIUS Groups the authenticated user belongs to.

2 Configure Connectra for Authentication by SafeWord PremierAccess

When SafeWord is selected as the RADIUS server the following three configuration steps must be performed in Connectra. It is recommended that these steps be performed in the following order:

- A. Identify SafeWord as the RADIUS server. Go to *Users and Groups > Authentication* and select *RADIUS Server* (Fig.1).
 - a. Check the *Use RADIUS* box.
 - b. Host Name/IP - enter the host name or IP address of the SafeWord PremierAccess server.
 - c. Server Port - enter the RADIUS port number. By default it is 1812 for Widows and 1645 for Solaris. The port number you select here must be the same you will enter for PremierAccess in step 3-A.
 - d. Version – leave as *RADIUS version 1.0*.
 - e. Shared Secret - enter and confirm a random string from 1 to 15 characters. You must enter this same string in PremierAccess in steps 3-A.
 - f. Click *Apply*.

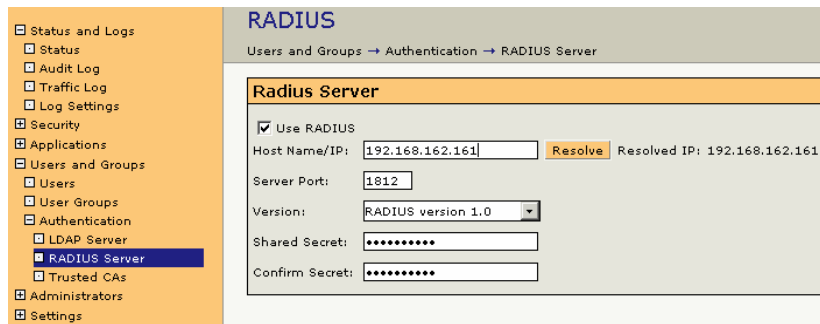


Fig. 1

- B. Create a user named *generic**. Go to *User and Groups > User and* click on *New* (Fig. 2) and enter the following:
 - a. Login Name - enter **generic***.
 - b. Authentication Schema - select RADIUS.
 - c. Click *Apply*.

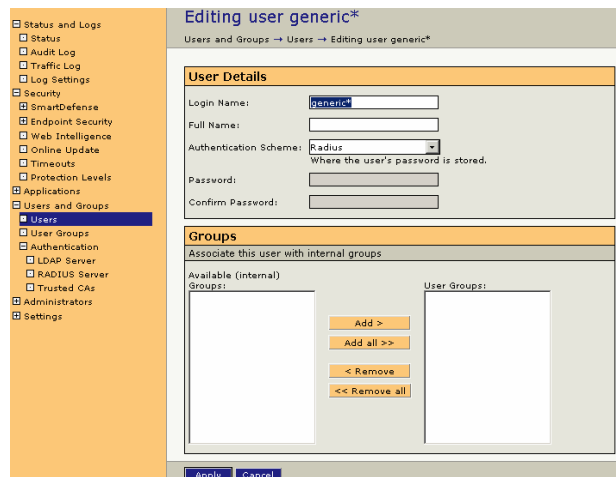


Fig. 2

C. Create RADIUS user groups. Create as many RADIUS Groups as your security policy requires and assign each group their access rights. RADIUS groups, by default, are mapped to the class attribute of the RADIUS user. For example, if the attribute value is managers, then you must create a RADIUS group in Connectra, with the name *managers*. Note that a user can belong to multiple RADIUS Groups. After a successful authentication, PremierAccess will return to Connectra the names of the RADIUS Groups the user belongs to. PremierAccess will return each group name as a value for a RADIUS attribute. Unless specifically changed, Connectra, by default, uses RADIUS attribute #25 (Class). If the user belongs to only one RADIUS Group a single value for this RADIUS attribute will be returned. If the user belongs to multiple RADIUS Groups, then multiple values of this attribute will be returned. Each value can be a string of one to 256 characters.

If another RADIUS attribute must be substituted for attribute #25, for example attribute #11 (Filter Id), the change must be reflected in both Connectra and SafeWord. In Connectra do the following:

- Run cpstop.
- Using a text editor edit the file *\$FWDIR/conf/objects_5_0.C*. Search for the string *radius_groups_attr*, and change the value inside the brackets from 25 (Class attribute code) to the desired attribute, such as 11 (Filter-Id).
- Run cpstart.

In SafeWord change to the alternate attribute when entering RADIUS attribute values in the *users* file in step 3-F.

To create RADIUS Groups go to *Users and Groups > User Groups*, select *New*, then *RADIUS Group*. In the *Adding a new group* window (Fig. 3) enter the following:

- a. Group name - enter a descriptive name for the RADIUS group.
- b. Click *Apply*.



Fig. 3

3. Configure SafeWord PremierAccess

A. Install SafeWord PremierAccess. Install SafeWord PremierAccess following instructions in the *Installation Guide*. When prompted for a RADIUS client, identify

Connectra and specify its RADIUS port and shared secret. Both must match the assignments you made in step 2-A.

If you fail to enter these parameters during installation or want to change them later, you can do so by using the administrative GUI or by editing the *clients* file in the *RADIUSServer* sub-directory. For these changes to take effect you must stop and restart the RADIUS server.

After installation download and install any patches that may be available for this system. Patches are available for download at <http://www.securecomputing.com/index.cfm?sKey=246>

Next you must configure a user database. Using the PremierAccess administrative GUI enter those Connectra users that will be authenticated by PremierAccess and configure their user profiles for the desired authentication method. For strong authentication select token-generated, one-time passwords (passcodes) as the authentication method.

Upon a successful authentication, PremierAccess will return to Connectra a RADIUS attribute containing the names of the Connectra RADIUS Groups the user belongs to. Although there are a other ways to configure PremierAccess to accomplish this, the following method will be used as an example:

Create a role in PremierAccess for each permutation of RADIUS group memberships that are assigned to Connectra users. For example, in Fig. 4, all three Connectra users share the same permutation of RADIUS Groups. They all belong to the RADIUS Group *managers* and to the RADIUS Group *sales*. In PremierAccess these users will be assigned the same role: *Sales_Managers*. Link each role to an ACL and to an entry in the *users* file that identifies the RADIUS attributes that must be returned to Connectra (In our example: *managers* and *sales*).

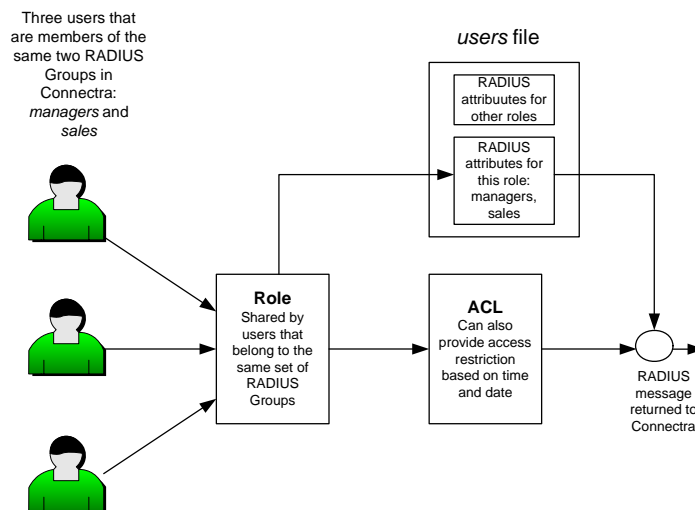


Fig. 4

B. Create a role. From the main console highlight the *Admin group* that contains the Connectra users and select *Insert > Role*. In the *Create a New Role* window select the *General* tab (Fig. 5) and enter the following:

- a. Role – enter a name that is easy to associate with the permutation of the RADIUS groups this role will represent, for example *Sales_Managers*.
- b. Admin Group – Leave as shown.
- c. Login ACL - For now leave as “*NONE CHOSEN*”. You will select an ACL after the ACL is created in the next step.
- d. Priority – select a desired value or leave as default.

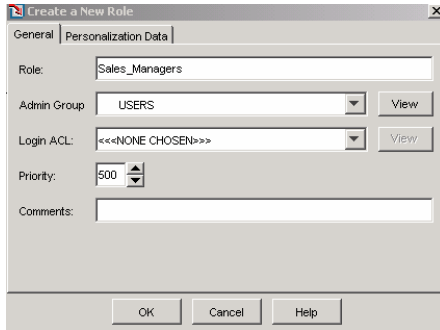


Fig. 5

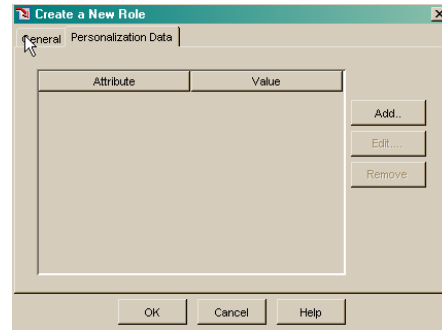


Fig. 6

Select the *Personalization Data* tab. In the *Personalization Data* window (Fig. 6) click on *Add*. In the *Add* window (Fig. 7) click on *Add New Personalization Data*. In the *Create a Personalization Data Attribute* window (Fig. 8) enter the following:

- a. Attribute - enter a descriptive name for the attribute that will be returned to Connectra, such as *RADIUS_attribute*.
- b. Select *Allow any value*
- c. Click *OK*

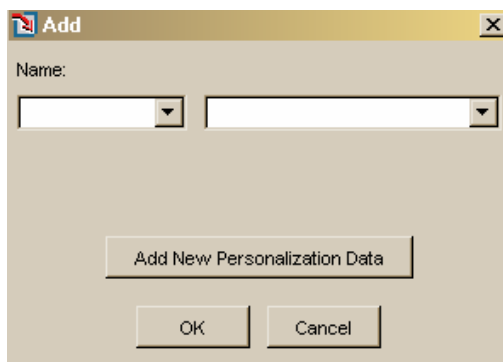


Fig. 7

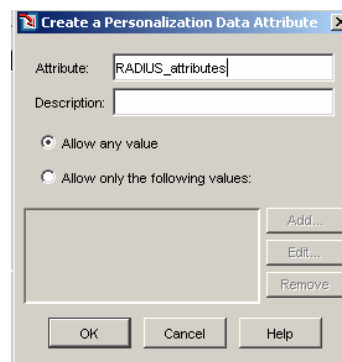


Fig. 8

In the refreshed *Add* window (Fig. 9), scroll down the *Name* menu and select the name of the Attribute you just created in the previous step.

- a. In the *Type a value* field enter the following:
`group=<group name>`

For <group name> substitute the name of the role you created (see Fig. 5). This name must also be entered in the users file in step 3-C.

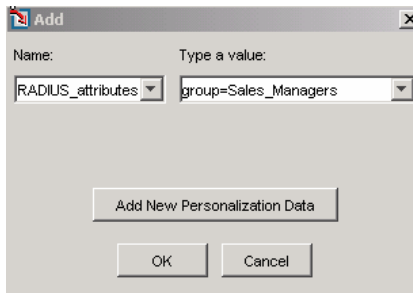


Fig. 9

- C. Create an ACL for each of the roles you created in step 2-B.** From the Admin Console select *Insert > ACL > Login*. In the *Create a New Login ACL* window (Fig. 10), enter the following:
- ACL - enter a name for this ACL
 - Select the appropriate Admin Group
 - Click on *New*

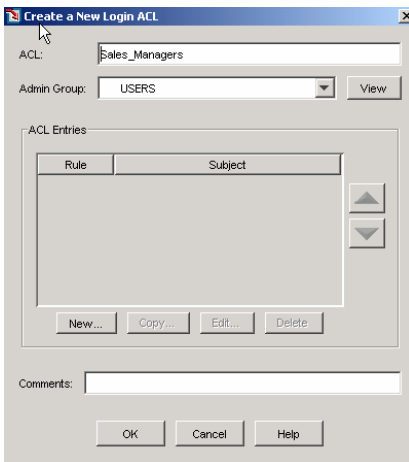


Fig 10

In *New ACL Entry* window (Fig 11) select the *Subject* tab and enter the following:

- Select *Some Users*
- Select *Role* and scroll down and select the role that will be associated with this ACL.

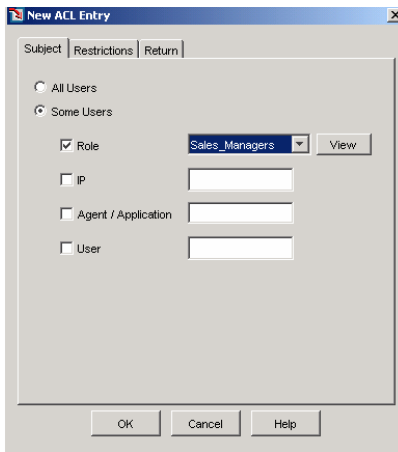


Fig 11

In the *Restriction* field of the *New ACL Entry* (Fig. 12):

- a. Select *Define a set of restrictions*.
- b. Select *Grant access if the user meets these restrictions*.
- c. Click on *Edit* and select the restrictions that will apply. Restrictions can be based on strength of the authenticator, time of day or a range of dates.

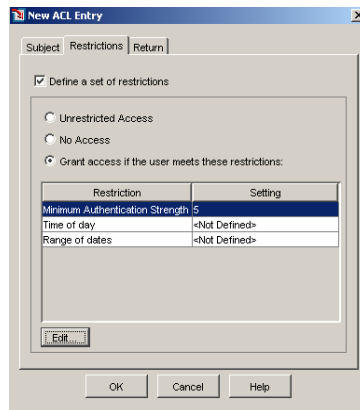


Fig 12

In the *Return* window of the *New ACL Entry* (Fig 13)

- a. Authentication status - select *Success*
- b. Select *Return a value on successful authentication*
- c. Select *Personalization Data*
- d. Scroll down and select the Personalization data you defined in step 2-B.
- e. Click OK

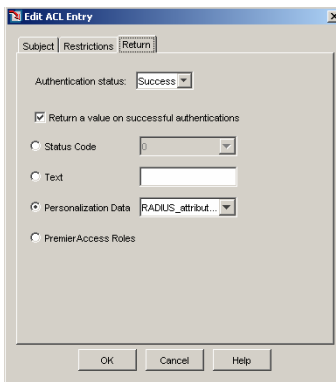


Fig 13

D. Link roles to ACLs. You must link each role you created to a corresponding ACL. Go to *Find > Roles*, and sequentially locate each role, double click on it and select *Edit*. In the *Edit Role* window (Fig. 14) select the appropriate Login ACL from the scroll down menu. Click *OK*.

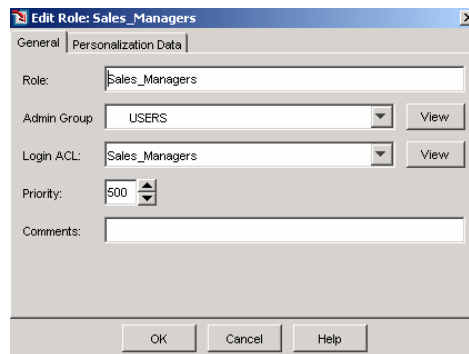


Fig. 14

E. Assign roles to users. Select each Connectra user, click on *Edit* and in the *Edit user* window (Fig. 15) assign the user one of the roles you created in step 2-B.

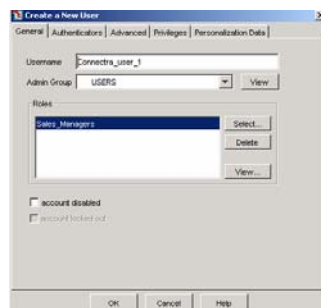


Fig 15

F. Edit the *users* file. Using a text editor, edit the *users* file located in the *PremierAccess/SERVERS/RADIUS/RADIUServer* directory (Partial view of the file is shown in Fig. 16).

- Add an entry for each role you create in step 2-A and give it the exact same name you entered in step 3-B (Fig. 9).
- Under the role list the RADIUS attributes and their values that must be returned for this role. By default Connectra expects this attribute to be #25 (Class). If another attribute is selected then the configuration change outlined in step 2-C must also be performed.

As an example, the bold entries in Fig 16, specify that for the role *Sales_Managers* two RADIUS attributes #25 (Class) will be returned: *managers*, *sales*.

```
#           Filter-Id = Dialin

Sales_Managers
    Class=managers
    Class=sales

DEFAULT    User-Password = "SAFWORD"
           Service-Type = Framed,
           Framed-Protocol = PPP,
           Framed-IP-Address = 10.20.0.1,
           Framed-IP-Netmask = 255.255.255.0

#
```

Fig. 16