



## Cloudezza RADIUS Manual

(c) Cloudezza, Inc., [www.cloudezza.com](http://www.cloudezza.com) 2013

Version 1.16

[Chapter 1: 60-second lessons.](#)

[Lesson 1: Create a user and a group.](#)

[Lesson 2: Create a simple PAP server.](#)

[Lesson 3: Create a simple WPA2-Enterprise/PEAP server.](#)

[Lesson 4: Restrict Client access by source IP addresses.](#)

[Lesson 5: Enable Two-factor authentication.](#)

[Lesson 6: Let users change and reset passwords.](#)

[Lesson 7: Manage RADIUS attributes.](#)

[Lesson 8: Create guest login.](#)

[Lesson 9: Authenticate users using Google Apps.](#)

[Section 2: Users and Groups.](#)

[2.1 Users.](#)

[2.2 Bulk User Import.](#)

[2.3 User Groups.](#)

[2.4 External User Groups.](#)

[2.5 Google Apps authentication.](#)

[Section 3: Virtual RADIUS Servers.](#)

[3.1 RADIUS Server Basics.](#)

[3.2 Creating a Virtual RADIUS Server - Simple Config.](#)

[3.3 Creating a Virtual RADIUS Server - Advanced Config.](#)

[3.3 Permitting user groups to authenticate against the server.](#)

[Section 4: Guest access.](#)

[4.1 Guest Users.](#)

[4.2 Access Card sheets.](#)

[Section 5. Two-factor authentication.](#)

[5.1 Two-factor authentication basics.](#)

[5.2 Enabling Two-Factor Authentication for a particular user.](#)

[5.3 Installing Google Authenticator.](#)

[5.4 Scanning Bar Code into Google Authenticator.](#)

[5.5 Using Google Authenticator to log in to the Web Interface.](#)

[5.6 Using Google Authenticator to authenticate against a Virtual RADIUS server.](#)

[Section 6. Securing Access To a Virtual RADIUS Server.](#)

[6.1 Introduction to Source IP Addresses.](#)

[6.2 Defining Source IP addresses.](#)

[6.3 Adding Source IP addresses to RADIUS Server.](#)

[Section 7. Using Vendor Specific Attributes.](#)

[7.1 Vendor Specific Attribute Basics.](#)

[7.2 User, Group and Virtual Server attributes.](#)

[7.3 Adding a Vendor Specific Attribute to a User, Group or Virtual Server.](#)

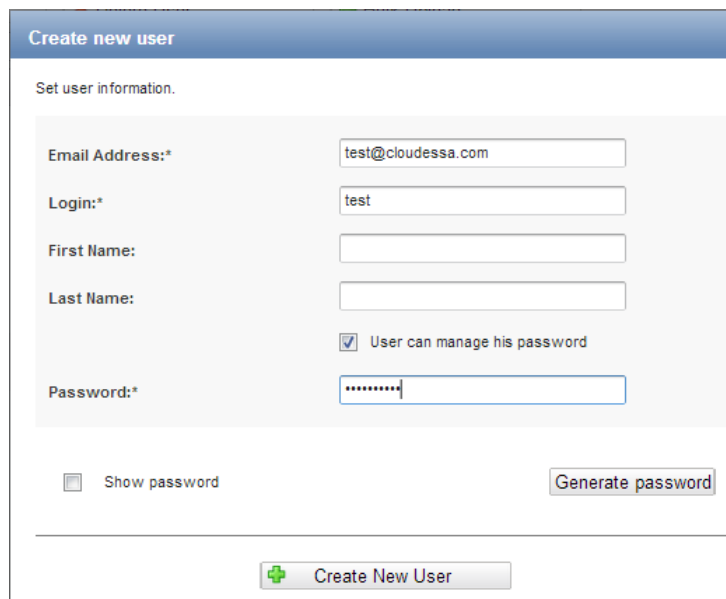
[8.1 IP Pool basics.](#)

# Chapter 1: 60-second lessons.

## Lesson 1: Create a user and a group.

In this lesson you create a group of RADIUS users, and add at least one user to this group. You'll need this for all other lessons.

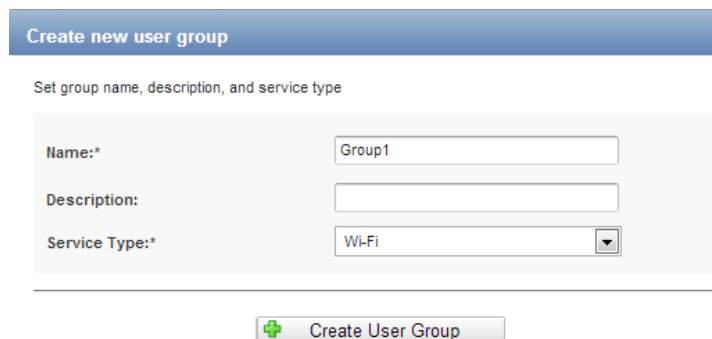
First create a user:



The screenshot shows a web form titled "Create new user". The form is divided into two main sections. The top section, "Set user information.", contains several input fields: "Email Address:\*" with the value "test@cloudessa.com", "Login:\*" with the value "test", "First Name:" (empty), "Last Name:" (empty), and "Password:\*" (masked with dots). There is a checkbox labeled "User can manage his password" which is checked. Below these fields are two buttons: "Show password" (disabled) and "Generate password". The bottom section of the form features a single button labeled "Create New User" with a green plus icon.

- Go to **Users** and click **Create**
- Specify login as *test*, email as *test2@cloudessa.com* and password as *mypassword*
- Click **OK**

Now create a group:



The screenshot shows a web form titled "Create new user group". The form is divided into two main sections. The top section, "Set group name, description, and service type", contains three input fields: "Name:\*" with the value "Group1", "Description:" (empty), and "Service Type:\*" with a dropdown menu showing "Wi-Fi". Below these fields is a single button labeled "Create User Group" with a green plus icon.

- Go to **User Groups** and click **Create**
- Specify name as *Group1*
- Select the service this group will be using, such as *Wi-Fi*
- Click **OK**

Now add the user to the group:

The screenshot shows the 'User Groups' management interface. At the top, there are buttons for 'Create User Group' and 'Delete User Group'. Below that is a 'Filter by:' dropdown menu set to 'Name' and a search input field. A table lists the user groups, with 'group1' selected. Below the table, there are tabs for 'Manage Group', 'VLAN', 'Users', 'Attributes', and 'IP Pool'. The 'Users' tab is active, showing 'Add User' and 'Remove' buttons. A table below lists the users in the group:

	Email	Login	Firstname	Lastname	Role
<input type="checkbox"/>	test2@cloudessa.com	test2	Test	Test	Regular user

- Select *Group1*
- Go to **Users** tab.
- Click **Add user** and select user *test*
- Click **OK**

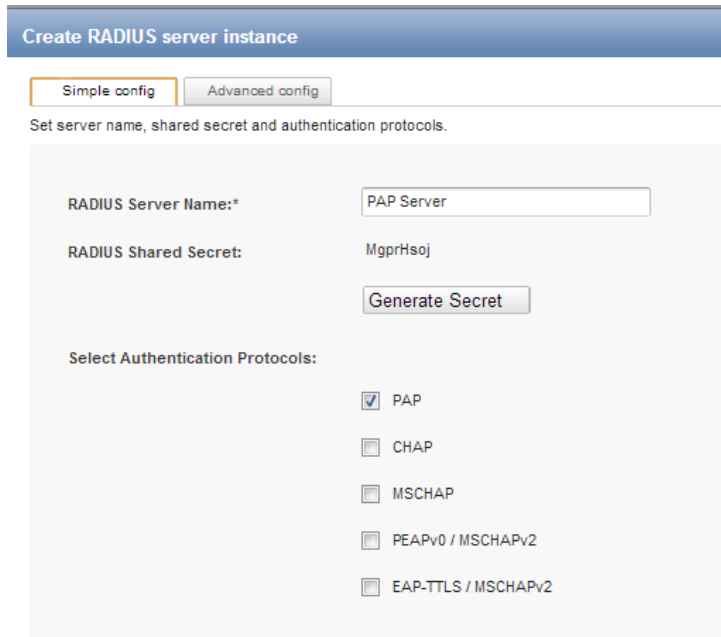
The user will then be displayed as added to the group.

Now we have created user *test* which is a member of *Group1*.

## Lesson 2: Create a simple PAP server.

In this lesson we create a simple authentication server that authenticates users using PAP protocol.

First lets create a virtual RADIUS server:

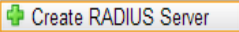
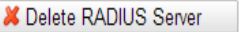


The screenshot shows a web-based configuration interface for creating a RADIUS server instance. At the top, there is a blue header bar with the text "Create RADIUS server instance". Below this, there are two tabs: "Simple config" (which is active) and "Advanced config". Under the "Simple config" tab, there is a sub-header "Set server name, shared secret and authentication protocols." The main configuration area contains the following fields and options:

- RADIUS Server Name:\*** A text input field containing "PAP Server".
- RADIUS Shared Secret:** A text input field containing "MgprHsoj".
- Generate Secret:** A button located below the shared secret field.
- Select Authentication Protocols:** A section with five checkboxes:
  - PAP
  - CHAP
  - MSCHAP
  - PEAPv0 / MSCHAPv2
  - EAP-TTLS / MSCHAPv2

- Go to **Virtual Servers**, click **Create**
- In the pop-up window set server name to **PAP Server** and protocol to **PAP**
- Click **OK**. Now the server is created
- Now click on the server entry to see the **IP address**, the **shared secret** as well as the **authentication and accounting port numbers** for the server. You need this information to configure your RADIUS client

**Virtual RADIUS Servers**

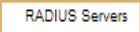



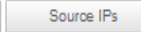
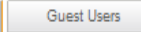

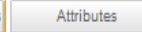



Filter by: Server Name  Page: 1 / 1

Server Name	User Groups	Source IPs	Server IP	Authentication Port	Accounting Port
PAP Server	0	0	23.23.234.126	1256	1257

---

**Virtual RADIUS Server : PAP Server**

Virtual Server Name: PAP Server


RADIUS Server IP: 23.23.234.126

Authentication Port: 1256

Accounting Port: 1257

RADIUS Shared Secret: MgprHsoj

Disable IP Filtering



Now we need to specify user groups that have access to the RADIUS server.

- Select *PAP Server* in the **Virtual Servers** table
- Go to **User Groups** tab
- Click **Add Group** and select *Group1* (we have created it in Lesson 1)

**Virtual RADIUS Servers**

Help

Filter by: Server Name  Page: 1 / 1

Server Name	User Groups	Source IPs	Server IP	Authentication Port	Accounting Port
PAP Server	1	0	23.23.234.126	1256	1257

---

**Virtual RADIUS Server : PAP Server**

Name	Description	Service Type
<input type="checkbox"/> group1		Wi-Fi

Now let us specify that the server will accept PAP requests from all sources.

- Select *PAP Server* in the **Virtual Servers** table
- Click **Edit**
- Set **Disable IP filtering** checkbox

**Virtual RADIUS Server : PAP Server**

**Virtual Server Name:** PAP Server

**RADIUS Server IP:** 23.23.234.126

**Authentication Port:** 1256

**Accounting Port:** 1257

**RADIUS Shared Secret:** VvIFq8ZY

Disable IP Filtering

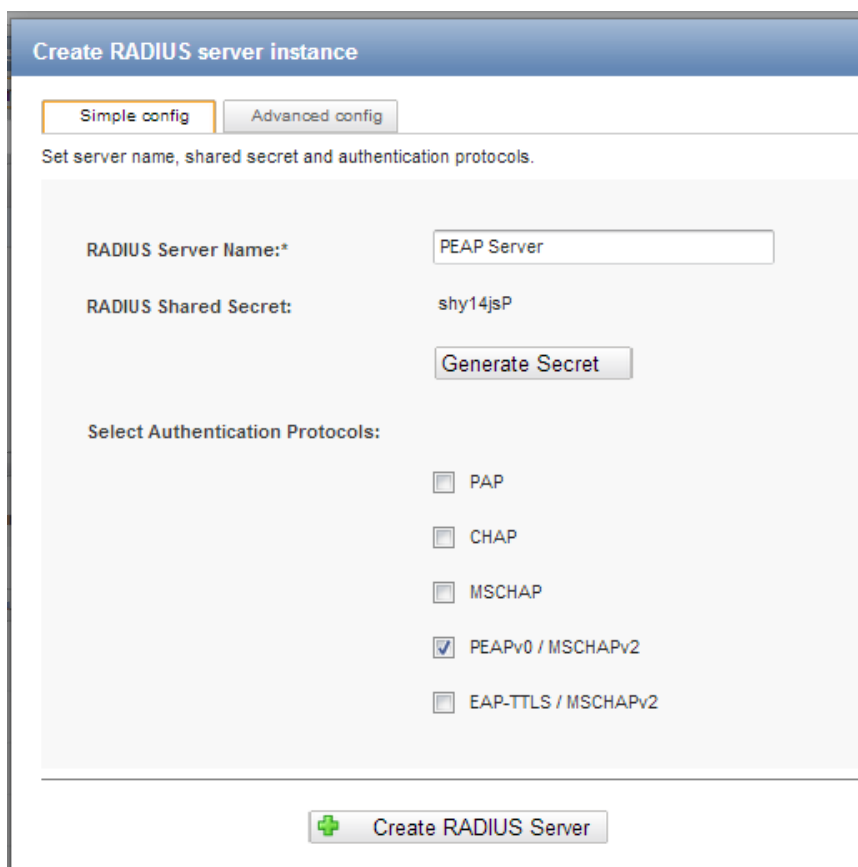
Now the PAP server is running and authenticating users from `Group1`.

## Lesson 3: Create a simple WPA2-Enterprise/PEAP server.

PEAP is a protocol widely used to secure Wi-Fi.

In this lesson we create a simple PEAP server.

- Go to **Virtual Servers**, click **Create**
- In the pop-up window set server name to *PEAP Server* and protocol to *PEAPv0/MSCHAPv2*
- Click **OK**. Now the server is created
- Now click the server entry to see the **IP address** as well as the **authentication and accounting port numbers** for the server. You need this information to configure your RADIUS client



The screenshot shows a web-based configuration interface titled "Create RADIUS server instance". It has two tabs: "Simple config" (selected) and "Advanced config". Below the tabs, there is a heading "Set server name, shared secret and authentication protocols." The form contains the following fields and options:

- RADIUS Server Name:\*** A text input field containing "PEAP Server".
- RADIUS Shared Secret:** A text input field containing "shy14jsP".
- Generate Secret:** A button to generate a new shared secret.
- Select Authentication Protocols:** A section with five checkboxes:
  - PAP
  - CHAP
  - MSCHAP
  - PEAPv0 / MSCHAPv2
  - EAP-TTLS / MSCHAPv2

At the bottom of the form is a large button with a green plus icon and the text "Create RADIUS Server".

Now we need to specify user groups that can authenticate against the RADIUS server.

- Select *PEAP Server* in the **Virtual RADIUS Server** table
- Go to **User Groups** tab
- Click **Add Group** and select *Group1* (we have created it in Lesson 1)



**Virtual RADIUS Servers**

Filter by:

Page: 1 / 1

Server Name	User Groups	Source IPs	Server IP	Authentication Port	Accounting Port
PEAP Server	1	0	23.23.234.126	1258	1259
PAP Server	1	0	23.23.234.126	1256	1257

**Virtual RADIUS Server : PEAP Server**

	Name	Description	Service Type
<input type="checkbox"/>	group1		Wi-Fi

Now lets specify that the server will accept PEAP requests from all sources.

- Select *PEAP Server* in the server table
- Click **Edit**
- Set **Disable IP filtering**

## Virtual RADIUS Server : PAP Server

RADIUS Servers	Auth Protocols	User Groups	Ext User Groups
Virtual Server Name:	PAP Server		
RADIUS Server IP:	23.23.234.126		
Authentication Port:	1256		
Accounting Port:	1257		
RADIUS Shared Secret:	VvIFq8ZY		
	<input checked="" type="checkbox"/> Disable IP Filtering		
			

Now the PEAP server is running and authenticating users from Group1.

## Lesson 4: Restrict access by source IP addresses.

For security reasons it is important to restrict access to the server to a set of allowed source IP addresses.

In this lesson we learn how to restrict access to Cloudessa by source IP address.

The server will then only accept a RADIUS request if it comes from one of the allowed source IP addresses.

Note: if your RADIUS client or Network Access Server is behind a firewall, then the source IP address that Cloudessa will see is the IP address of the firewall.

Let us assume that the ip address of your firewall is 20.21.22.23.

First lets create a source IP address.

- Go to **Src IP Addresses**, click **Create**
- In the pop-up window set the IP address to *20.21.22.23*
- Click **OK**. Now the source IP address is created

Now we need to add this source IP address as allowed for the *PAP server* we created in Lesson 2.

- Select *PAP Server* in the server table
- Click *Edit*, unset **Disable IP filtering** checkbox, and click **Save**
- Go to **Src IP Addresses** tab
- Click **Add src IP address**, and select *Gateway1*

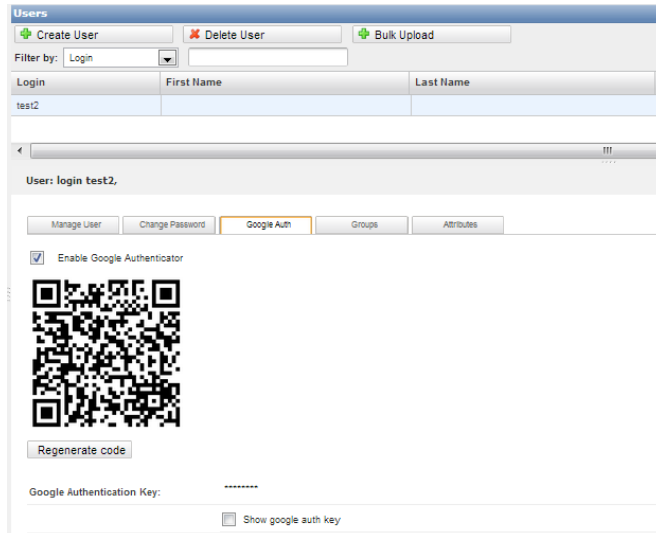
IP Address	Description
<input checked="" type="checkbox"/> 10.11.12.13	

Now *PAP Server* is running and accepting only requests that come from the ip address *20.21.22.23*.

## Lesson 5: Enable Two-factor authentication.

To enable two-factor authentication for user *test*.

- Select user *test* in the **Users** panel
- Select **Google Auth** tab
- Set **Enable Google Authenticator**. A bar code will be generated



Now one needs to setup the smartphone for the user.

- Download Google Authenticator app for
  - iPhone <http://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8>
  - Android <https://play.google.com/store/search?q=google+authenticator>
  - WindowsPhone <http://www.windowsphone.com/en-US/apps/021dd79f-0598-e011-986b-78e7d1fa76f8>
  - Blackberry <http://m.google.com/authenticator>
- Scan user barcode into Google Authenticator app
- The app will start displaying temporary six-digit codes

To perform two-factor authentication into Cloudessa RADIUS

- use the password composed of your regular password and the six digit code, separated by a comma

As an example:

**login:** *test*

**password:** *mypassword,315425*

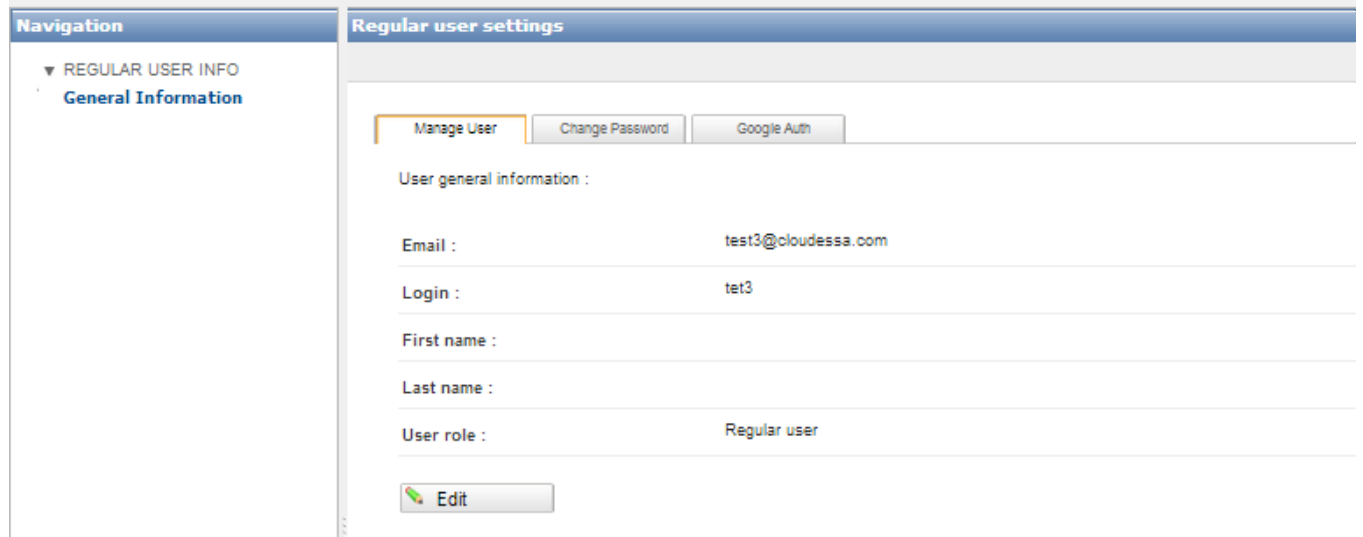
## Lesson 6: Let users change and reset passwords.

Cloudessa enables regular RADIUS users to change their passwords using a simple web interface.

If you do not want a particular user to be able to change or reset his password, you can unset **Allow user to manage his password** checkbox in the user settings tab.

To access the simple web interface for user `test` created in Lesson 1.

- Go to Cloudessa login page <https://app.cloudessa.com/account/login>
- Enter user email *test@cloudessa.com`* and password *mypassword*
- You will be presented with the simple web interface panel.



The screenshot shows the 'Regular user settings' page in the Cloudessa application. On the left is a navigation menu with 'REGULAR USER INFO' expanded to show 'General Information'. The main content area has three tabs: 'Manage User' (selected), 'Change Password', and 'Google Auth'. Below the tabs, the 'User general information' section displays the following details:

Email :	test3@cloudessa.com
Login :	tet3
First name :	
Last name :	
User role :	Regular user

At the bottom of the form is an 'Edit' button with a pencil icon.

To change user password

- Select to the **Set Password** panel
- Set the new password

If the user needs to reset her password

- User clicks on the `Reset password` link included in **Cloudessa login page** <https://app.cloudessa.com/account/login>

- Password reset instructions are emailed to the user

## Lesson 7: Manage RADIUS attributes.

Cloudessa lets you set RADIUS attributes that the virtual server will return in RADIUS response messages. You can set return attributes for a server, a user group or a particular user.

As an example, to return *Framed-IP-Address* attribute value of *12.13.14.15* for user *test* created in Lesson 1

- Select user *test* in the **Users** panel
- Select **Attributes** tab and click **Add**
- Select *RFCs* dictionary
- Select *Framed-IP-Address* attribute and set attribute value to *12.13.14.15*
- Click **OK**

Note: for a particular authentication request, Cloudessa RADIUS first identifies the user, the user group and the virtual RADIUS server, and then adds up the corresponding three sets of attributes. If the same attribute value is set for the user, the user group and/or the RADIUS server, then the user group attribute overrides the server attribute, and the user attribute overrides the user group attribute.

## Lesson 8: Create guest login.

To give your guest *guest1@gmail.com* a temporary login into the *PEAP server* created in Lesson 3.

- Go to the **Guest Users** tab
- Click **Create Guest User**
- Enter guest email *guest1@gmail.com*
- Set the **Expiration date** to, e.g., *May 1, 2013*
- Click **OK**

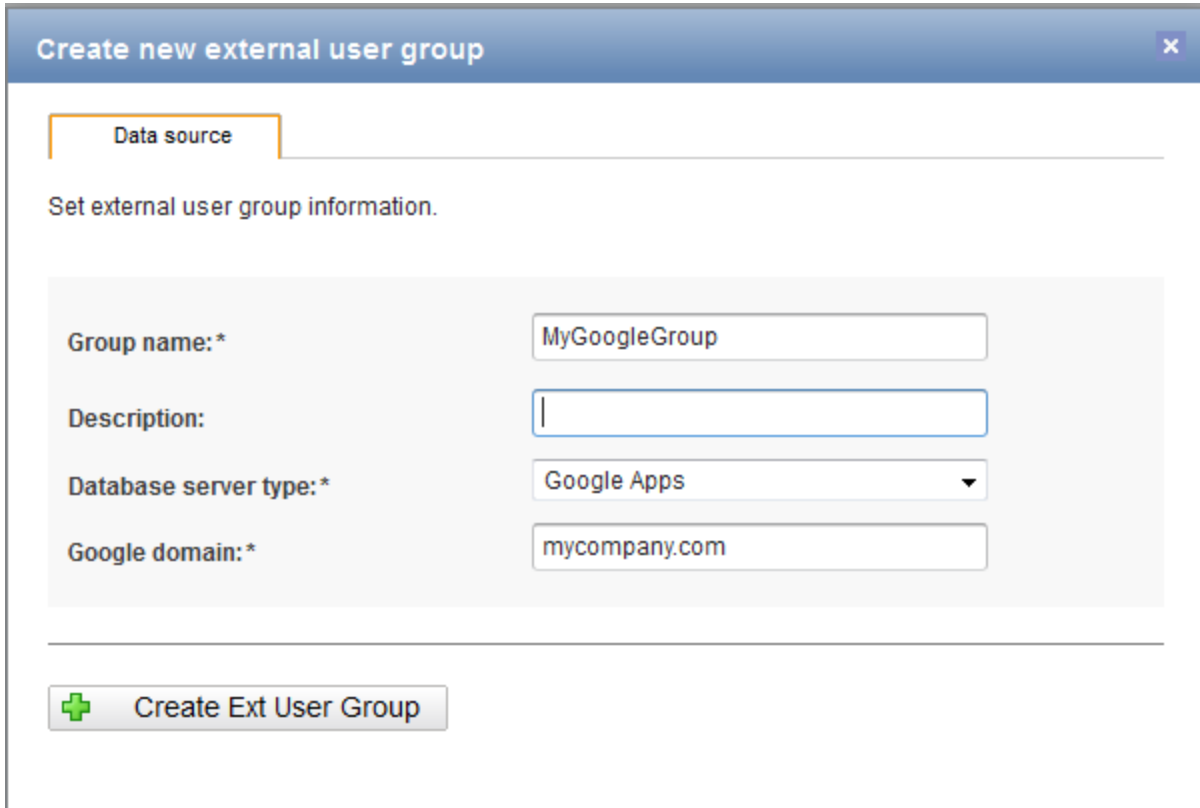
## Lesson 9: Authenticate users using Google Apps.

In this lesson you learn how to authenticate users using their Google Apps usernames and passwords.

Lets suppose you have Google Apps for the domain *mycompany.com*. You want to give your Google Apps users access into the *PAP server* created in Lesson 4.

First create an external user group that will map to Google Apps

- Go to the **External User Groups** menu
- Click **Create Ext User Group**
- Type *MyGoogleGroup* as group name
- Choose *Google Apps* as **Database Server Type**
- Enter *mycompany.com* as **Google Domain**
- Click **Create Ext User Group**



Create new external user group

Data source

Set external user group information.

Group name:\* MyGoogleGroup

Description:

Database server type:\* Google Apps

Google domain:\* mycompany.com

+ Create Ext User Group

Second attach the group to the *PAP Server*

- Go to **Virtual RADIUS Servers**
- Select *PAP Server*
- Go to **Ext User Groups** tab
- Click **Add Group**
- Choose *Google* group

- Click **Add Group**

**Add group to RADIUS server** ✕

Select group that you want to add to RADIUS server

Filter by:

	Name	Description
<input type="checkbox"/>	Domain cloudessa	
<input type="checkbox"/>	Active Directory	Local Active Directory 2003
<input checked="" type="checkbox"/>	MyGoogleGroup	



## Section 2: Users and Groups.

### 2.1 Users.

Cloudessa supports the following user roles:

- *Primary Admin (root)* manages all Cloudessa features. Primary Admin can not be deleted.
- *Admins* manage all Cloudessa features, authenticate against virtual RADIUS servers and access the full web interface. An admin can be deleted by the primary admin. An admin can create another admin.
- *Users* can use Cloudessa RADIUS server for authentication, authorization and audit. They can also optionally manage their passwords through the web interface, if permitted by the administrator.
- *User Managers* can use Cloudessa RADIUS server for authentication , as well as create, remove and manage RADIUS users.
- *Guest Users* can have temporary guest access to the Cloudessa RADIUS server for authentication, authorization and audit.

Users have two important attributes:

- *email* is used to identify the users to the web interface
- *RADIUS login* is used to identify the user during the RADIUS authentication session

If the administrator sets the “*User Can Manage his password*” flag for the user, the user can use web interface to change and reset her password.

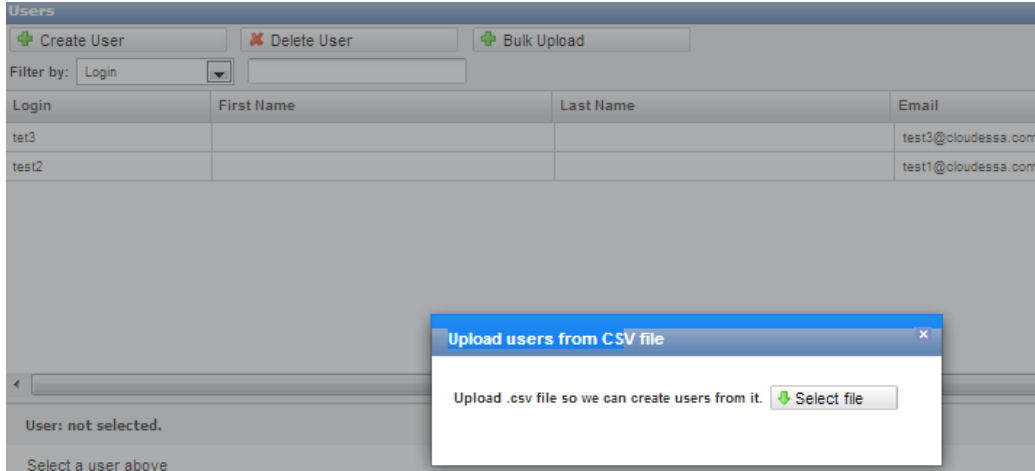
Note that the same password is used both for the web interface and for the RADIUS server.

### 2.2 Bulk User Import.

Cloudessa allows admins to perform bulk user import and creation using a CSV file. The CSV file shall contain a set of lines in the following format “*username, password*”.

To bulk upload users, one shall

- Click the **Bulk Upload** button in the web interface
- Choose the CSV file to upload
- Click **OK**



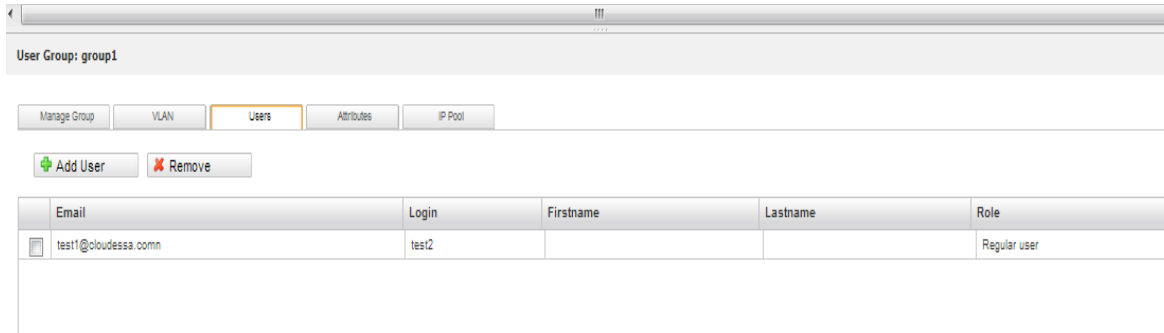
## 2.3 User Groups.

A user group includes group name, description, and the service type that this group is provided access to. Currently the available services are *Wi-Fi*, *VPN*, *SSH*, *Local login*, and *Other*.

To create a group one clicks on the **Create User Group** button in the **User Groups** menu.

The screenshot shows the 'Create new user group' form. It has a blue header with the text 'Create new user group'. Below the header is the instruction 'Set group name, description, and service type'. The form contains three input fields: 'Name:\*' with an empty text box, 'Description:' with an empty text box, and 'Service Type:\*' with a dropdown menu showing 'Wi-Fi'. At the bottom of the form is a green button with a plus sign and the text 'Create User Group'.

The user membership in the group can be managed from the **Users** tab.



When a user group is added to a virtual RADIUS server, all users in this group are permitted to authenticate against this server and can access services protected by the server.

There is one default group “All Users”. This group includes all users.

## 2.4 External User Groups Overview.

External User Groups are used to authenticate against external user stores, such as Google Apps, LDAP, Active Directory, or databases such as MySQL, Oracle or DB2.

Each External User Group corresponds to a particular external user store.

- When multiple external user groups are added to a virtual server and a user tries to authenticate, then all internal and external groups are tried in a sequence.
- If at least one group includes the user and authentication against this group succeeds then the user is allowed to authenticate against the virtual server.

This means that in order for the user authentication to succeed success at least one external or internal group need to return success for authentication of this user.

To create an external user group,

- Go to **External User Groups** menu
- Click the **Create Ext User Group** button.

**Create new external user group** [X]

Data source | User config mapping

Set external user group information.

Group name:\* MyGroup

Description:

Database server type:\* MySQL

Host name or IP address:\*

Port:\* 3306

DB name:\*

User name:\*

Password:

Show password

Test Connection | Next >

Depending on the user store, different parameters are required to set up an External User Group.

## 2.5 External User Groups: SQL Databases

For SQL databases, such as MySQL, Oracle or DB2 the following parameters are required:

- Host name - domain name or IP address of the database server
- Port - port on the database server, the default port is preset (such as 3006 or MySQL)
- DB Name - name of the database
- User name - username to connect to the database
- Password - password used to connect to the database

## Create new external user group

Data source

User config mapping

Set external user group information.

Group name:*	<input type="text"/>
Description:	<input type="text"/>
Database server type:*	MySQL <input type="button" value="v"/>
Host name:*	<input type="text"/>
Port:*	3306
DB name:*	<input type="text"/>
User name:*	<input type="text"/>
Password:	<input type="text"/>

Show password

## 2.6 External User Groups: Active Directory.

For Microsoft Active Directory, the following parameters are required

- *Host name* - domain name or IP address of the Active Directory host
- *Port* - port on the Active Directory host, the default is 445
- *Domain* - Windows domain
- *User name* - user name to connect to Active Directory
- *Password* - password to connect to Active Directory

## Create new external user group

Data source

Set external user group information.

Group name:*	<input type="text"/>
Description:	<input type="text"/>
Database server type:*	Active directory <input type="button" value="v"/>
Host name:*	<input type="text"/>
Port:*	445
Domain:*	<input type="text"/>
User name:*	<input type="text"/>
Password:	<input type="password"/>

Show password

Test Connection

## 2.7 External User Groups: Google Apps

Cloudessa allows to create an external user group that is mapped to all users from a Google Apps Domain. This means that you can use Google Apps usernames and passwords to authenticate your VPN and Wi-Fi users using PAP and EAP-TTLS protocols.


To create an external user group for Google Apps, go to **External User Groups** click the **Create Ext User Group** button and choose *Google Apps* as an external user group type.

### Create new external user group ✕

**Data source**

Set external user group information.

Group name:*	<input type="text" value="MyGoogleGroup"/>
Description:	<input type="text"/>
Database server type:*	<input type="text" value="Google Apps"/>
Google domain:*	<input type="text" value="mycompany.com"/>

 **Create Ext User Group**

The following parameters are required

- **Google Domain** - domain name for your Google Apps such as *mycompany.com*

You can use Google Apps authentication with PAP, and EAP-TTLS/PAP protocols. Create a Virtual RADIUS server with PAP or EAP-TTLS/PAP protocols enabled and attach the external user group to this server.

- PAP protocol is normally used to authenticate your VPN users
- 
- EAP-TTLS/PAP is used to to authenticate your Wi-Fi users.

Windows 8, Android, Linux, and iOS support EAP-TTLS/PAP protocol for Wi-Fi connections. For older versions of Windows you need to use a third party EAP-TTLS client, such as

- [www.securew2.com](http://www.securew2.com) (commercial) or
- Intel Pro Wireless (free client for Intel Centrino platform).

## Section 3: Virtual RADIUS Servers.

### 3.1 RADIUS Server Basics.

Cloudessa allows to create multiple Virtual RADIUS servers. Each virtual RADIUS server corresponds to what used to be a dedicated software or hardware RADIUS server.

Each Virtual RADIUS Server is described by three parameters

- *RADIUS Authentication Port* - the server listens on this port for incoming authentication requests
- *RADIUS Accounting Port* - the server listens on this port for incoming accounting requests
- *RADIUS Secret* - communications with the server are protected using this secret.

To configure your Access Point, Network Access Server, VPN or other RADIUS-enabled hardware or software to communicate with Cloudessa, you need to enter these three pieces of information into your RADIUS-enabled hardware or software.

### 3.2 Creating a Virtual RADIUS Server - Simple Config.

To create a Virtual RADIUS Server use **Create RADIUS Server** Dialog in **Virtual RADIUS Servers** menu.

The **Simple Config** tab includes widely used protocols:

*PAP*, *CHAP*, and *MSCHAP* are the protocols frequently used by hardware network devices, such as VPNs and Routers.

*PEAPv0/MSCHAPv2* is widely used EAP-based protocol used to secure WiFi.

*EAP-TTLS/MSCHAPV2* is another widely used EAP-based protocol used to secure WiFi.

To create a Virtual RADIUS Server

- Click **Create Virtual RADIUS Server**
- Specify server name
- *RADIUS secret* is automatically generated, you can regenerate it by pressing **Generate Secret** button.
- Choose protocol
- Click **Create RADIUS Server** button.



### Create RADIUS server instance

Simple config | Advanced config

Set server name, shared secret and authentication protocols.

RADIUS Server Name:\*

RADIUS Shared Secret: 2%HbfpuB

Select Authentication Protocols:

- PAP
- CHAP
- MSCHAP
- PEAPv0 / MSCHAPv2
- EAP-TTLS / MSCHAPv2

### 3.3 Creating a Virtual RADIUS Server - Advanced Config.

The Advanced Config tab includes all protocols supported by Cloudessa

*PAP*, *CHAP*, and *MSCHAP* are the protocols frequently used by hardware network devices, such as VPNs and Routers.

Cisco *LEAP* is EAP-based protocol designed by Cisco, which is used to secure Wi-Fi.

*PEAPv0* is widely used EAP-based protocol used to secure Wi-Fi. Once you select *PEAPv0* you can select *MD5* or *MSCHAPv2* as inner authentication protocols.

*EAP-TTLS* is another widely used EAP-based protocol used to secure Wi-Fi. Once you select *PEAPv0* you can select *PAP*, *CHAP*, *MSCHAP*, *MSCHAPv2*, and *MD5* as inner authentication protocols.

*EAP-TTLS / MSCHAPv2* is another widely used EAP-based protocol used to secure Wi-Fi.

To create a virtual RADIUS server:

- Click **Create Virtual RADIUS Server**
- Select server name
- *RADIUS secret* is automatically generated, you can regenerate it by pressing **Generate Secret** button.
- Choose protocol
- Click **Create RADIUS Server** button.

### Create RADIUS server instance

Simple config

Advanced config

Set server name, shared secret and authentication protocols.

RADIUS Server Name:\*

RADIUS Shared Secret:

XrC8e3WW

Generate Secret

Select Authentication Protocols:

MSISDN

PAP

CHAP

MSCHAP

Cisco LEAP

PEAPv0

EAP-TTLS

### 3.3 Permitting user groups to authenticate against the server.

Once you created a Virtual RADIUS server, you need to specify which user groups (internal or external) can authenticate against this server.

To add a user group to a Virtual RADIUS server server.

- Select the server in the **Virtual RADIUS Servers** table
- Select the **User Groups** tab
- Click **Add Group** button

Note: in order for the user to be able to authenticate against a virtual RADIUS server, the user must belong to one of the user groups added to the server.

The screenshot shows the 'Virtual RADIUS Servers' management interface. At the top, there are buttons for 'Create RADIUS Server' and 'Delete RADIUS Server'. Below these is a 'Filter by:' dropdown set to 'Server Name' and a search input field. A pagination bar shows 'Page: 1 / 1'. The main table lists the following data:

Server Name	User Groups	Source IPs	Server IP	Authentication Port	Accounting Port
PEAP Server	1	1	23.23.234.126	1258	1259

Below the table, the interface shows the selected server 'Virtual RADIUS Server : PEAP Server'. A navigation bar includes tabs for 'RADIUS Servers', 'Auth Protocols', 'User Groups' (which is active), 'Ext User Groups', 'Source IPs', 'Guest Users', 'Access Card Sheets', and 'Attributes'. Below the tabs are 'Add Group' and 'Remove' buttons. The 'User Groups' section contains a table with the following data:

Name	Description	Service Type
group1		Wi-Fi

## Section 4: Guest access.


### 4.1 Guest Users.

A guest user is a temporary user account which has an expiration date. It can be used to provide access to a single virtual RADIUS server. Guest users are not allowed to access multiple servers.


To create a guest user, **Create New Guest User** dialog is used

#### Create new guest user

Set firstname, lastname, email address, expiration date and RADIUS server.

Firstname:	<input type="text"/>
Lastname:	<input type="text"/>
Email Address:*	<input type="text"/>
	<input checked="" type="checkbox"/> Send user login and password to his email
Expiration Date:	<input type="text" value="12/6/12"/> 
RADIUS Server:	<input type="text" value="PAP Server"/>

---

 **Create Guest User**

The *expiration date* is the last day when the user is allowed to login.

If the **Send user login and password to his email** checkbox is set, the temporary login and password are emailed to the user.

The RADIUS server is the server the guest user has access to. A guest user can only have access to a single virtual RADIUS server.

## 4.2 Access Card sheets.

An access card is a printable temporary access card that includes a temporary login and password. A sheet of access cards can be generated and then printed.

An access card can be used to provide access to a single virtual RADIUS server.


To create an access card sheet, user “Create New Access Card Sheet” dialog

### Generate new access card sheet

Set number of cards per sheet, validity period, and RADIUS server.

Validity Period:	<input type="text" value="15 minutes"/>
RADIUS Server:	<input type="text" value="PAP Server"/>
Number of Cards per Sheet: *	<input type="text" value="10"/>

---

 [Generate Access Card Sheet](#)

Once the user is authenticated the user has access for *Validity Period* which starts from the first time the user authenticated. The virtual server will send the *Session-Timeout* attribute back to the wireless Access Point or Network Access Server, in order to disconnect the user after the validity period expires. During the validity period the user may authenticate multiple times.

The *RADIUS server* is the server the card provides access to.

The *Number of cards per sheet* is the number of cards printed in a single card sheet.

## Section 5. Two-factor authentication.

### 5.1 Two-factor authentication basics.

CloudeSSA utilizes Google Authenticator smartphone application that generates temporary PIN codes each 30 seconds.

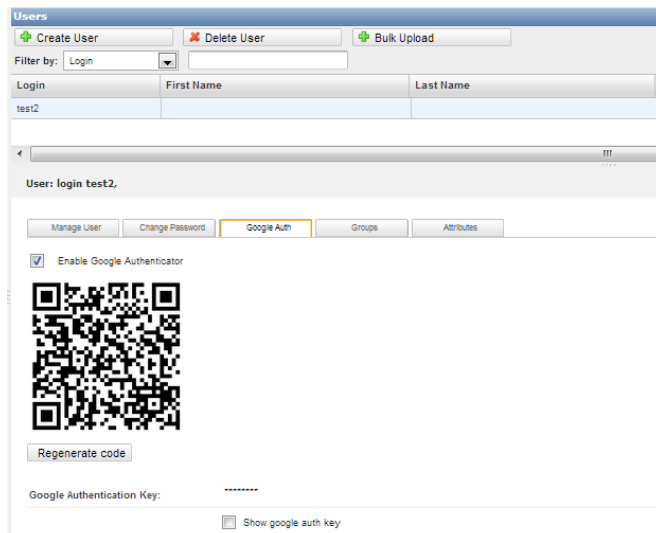
To authenticate to a virtual RADIUS server or to the Web UI, the user needs to possess two factors: the password and the temporary PIN. Therefore, without the smartphone the user can not authenticate, even if user password is stolen.

### 5.2 Enabling Two-Factor Authentication for a particular user.

Two-factor authentication is enabled on per-user basis. Once two-factor authentication is enabled for a particular user, both RADIUS access and Web UI access for this user will require the second authentication factor (PIN code).

To enable two-factor authentication for a particular user,

- select this user, select the **Google Authenticator** tab, and then select **Enable Google Authenticator**.
- User *secret master key* will be displayed as a bar code.
- This bar code needs to be scanned into the user smartphone (see the next section)



The *master key* can be regenerated by pressing **Regenerate Code** button.

As an option the *master key* can be displayed as a string. This feature is used for smartphones that do not have cameras and, therefore, can not scan the barcode. To display the code as a string, select the **Show Auth Key** checkbox.

## 5.3 Installing Google Authenticator.

To install Google Autnenticator on a smartphone:

- Download Google Authenticator app for  
iPhone <http://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8>  
Android <https://play.google.com/store/search?q=google+authenticator>  
WindowsPhone <http://www.windowsphone.com/en-US/apps/021dd79f-0598-e011-986b-78e7d1fa76f8>  
Blackberry <m.google.com/authenticator>
- Scan user barcode into Google Authenticator app
- The app will start displaying temporary six-digit codes

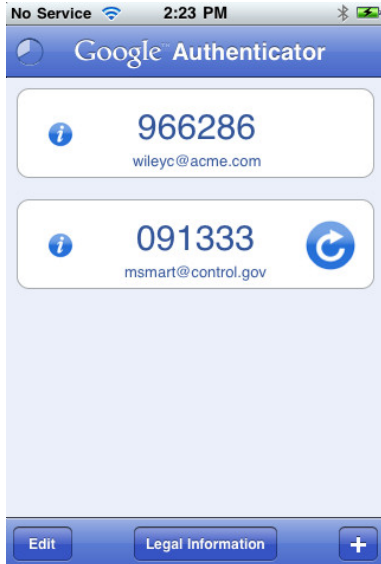
## 5.4 Scanning Bar Code into Google Authenticator.

To scan user barcode onto the Google Authenticator app

- open the Google authenticator app
- press + button, and then **Scan BarCode** button.
- Point the smartphone camera at the bar code, and press anywhere on the screen

If the smartphone does not include a camera, click + button, select **Time Based** and then manually type in the **Google Auth Key** string.

Once the bar code is scanned, the app will start displaying temporary 6-digit PINS.



## 5.5 Using Google Authenticator to log in to the Web Interface.

Once Google Authenticator is enabled for a particular user, two factor authentication is enabled both for RADIUS and for Web Interface.

To login into Web Interface

- Enter *username* and *password*
- A field prompting for the *PIN code* is displayed
- Read the *PIN code* from the smartphone and enter it

## 5.6 Using Google Authenticator to authenticate against a Virtual RADIUS server.

To authenticate against a virtual RADIUS server

- read the *temporary PIN* from the smartphone
- use in place of the regular password the following combination

*Regular Password then comma then temporary PIN*

For instance:

*MyPassword,123456*



## Section 6. Securing Access To a Virtual RADIUS Server.

### 6.1 Introduction to Source IP Addresses.

To make sure that only authorized users have access to a virtual RADIUS server, it is important to restrict access to a set of permitted source IP addresses.

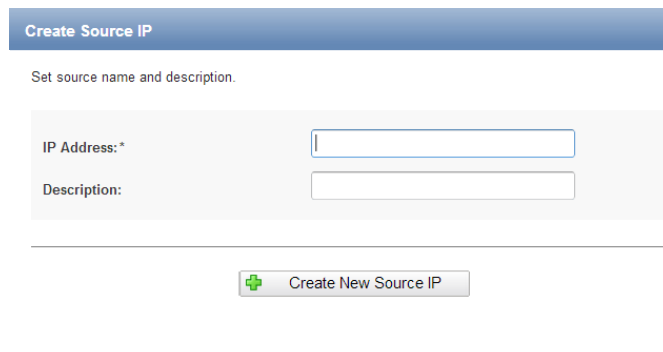
Typically an enterprise will use firewalls and gateways to separate the enterprise network from the public internet.

When Cloudezza receives a RADIUS request from a user authenticating to a Network Access Server (NAS), Wireless Access Point or enterprise VPN, the source IP address in the RADIUS request will typically be the source IP address of the firewall.

### 6.2 Defining Source IP addresses.

To secure your virtual RADIUS server, you first define the Source IP addresses for your organization.

- Obtain information about your organization public firewall and/or gateway IP addresses from your enterprise IT administrator
- For each IP address create a *Source IP address* entry using the **Create Source IP** dialog




Create Source IP

Set source name and description.

IP Address:\*

Description:

 Create New Source IP

### 6.3 Adding Source IP addresses to RADIUS Server.

To allow a request from a particular *Source IP address* to be authenticated against a particular RADIUS Server.

- Select the RADIUS server
- Select the **Source IP** tab

- Click **Add Source IP**
- Choose the *Source IP* to add

Virtual RADIUS Servers

Create RADIUS Server Delete RADIUS Server Help

Filter by: Server Name Page: 1 / 1

Server Name	User Groups	Source IPs	Server IP	Authentication Port	Accounting Port
PEAP Server	1	1	23.23.234.126	1258	1259
PAP Server	1	1	23.23.234.126	1256	1257

Virtual RADIUS Server : PEAP Server

RADIUS Servers Auth Protocols User Groups Ext User Groups **Source IPs** Guest Users Access Card Sheets Attributes

Add source IP Remove

IP Address	Description
10.11.12.13	

You can disable the Source IP address checking by setting the **Disable IP filtering** checkbox for the server.

RADIUS Servers Auth Protocols User Groups Ext User Groups

Virtual Server Name: PEAP Server

RADIUS Server IP: 23.23.234.126

Authentication Port: 1258

Accounting Port: 1259

RADIUS Shared Secret: shy14jsP

Disable IP Filtering

## Section 7. Using Vendor Specific Attributes.

### 7.1 Vendor Specific Attribute Basics.

Vendor-Specific Attributes are pieces of information that the RADIUS server returns back to the Network Authentication Server or Wireless Access Point after the user has authenticated. Each Vendor Specific Attribute includes a name, and then a value, which could be an integer, a string or another value type.

Vendor specific attributes are typically used to control user session, such as session expiration time or the virtual network (VLAN) that the user is placed into.

RADIUS-enabled hardware and software solutions coming from different vendors typically have sets of vendors specific attributes, this sets are denoted as *dictionaries*. Also, there are Vendor Specific Attributes specified in public standards and RFCs.

Cloudezza works to constantly update the sets of vendor specific attributes available in the product.

### 7.2 User, Group and Virtual Server attributes.

You can assign a Vendor Specific Attribute value to a user, a group of users or a virtual RADIUS server.

When an authentication request comes to authenticate a particular user against a particular server, and if the authentication request is successful, the vendor attributes are added up:

- Attributes of the user
- Attributes of all groups that the user has access to
- Attributes of the virtual server

The resulting attributes are then returned to in the authentication success message.

### 7.3 Adding a Vendor Specific Attribute to a User, Group or Virtual Server.

To add attribute to a user, a group, or a virtual server:

- Select the a user, a group or a virtual server
- Select *Dictionary*
- Select attributes you want to set and set the value for each attribute
- Click **Add**

## Add attributes

Select attributes you want to add.

Select attributes you want to add. RFCs

	Name	Value	Type
<input type="checkbox"/>	ARAP-Security		Integer
<input type="checkbox"/>	ARAP-Security-Data		String
<input type="checkbox"/>	ARAP-Zone-Access		Integer selection
<input type="checkbox"/>	Acct-Authentic		Integer selection
<input checked="" type="checkbox"/>	Acct-Delay-Time	100	Integer
<input type="checkbox"/>	Acct-Input-Gigawords		Integer
<input type="checkbox"/>	Acct-Input-Octets		Integer
<input type="checkbox"/>	Acct-Input-Packets		Integer
<input type="checkbox"/>	Acct-Interim-Interval		Integer

+ Add

Cancel

## Section 8. Using IP Pools.

### 8.1 IP Pool basics.

IP pools are used to assign IP addresses to devices which authenticate against a RADIUS Server.

IP addresses are assigned from pools of IP addresses. An IP address pool is defined by a range of IP addresses starting from a particular start address and ending with the end address.

An IP address is assigned to a device when the device is authenticated and is released when the RADIUS accounting message is received from the device specifying that the device disconnected.

To avoid IP address leakage one sets the IP entry maximum lifetime. After this time period, the IP address may be returned to the pool even if the accounting stop message was not received. The server will use this forced return strategy as the last resort, when there are no more free IP addresses available in the pool.

