Expedition

Admin Guide

Version 1.0

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 28, 2018

Contents

What is Expedition?

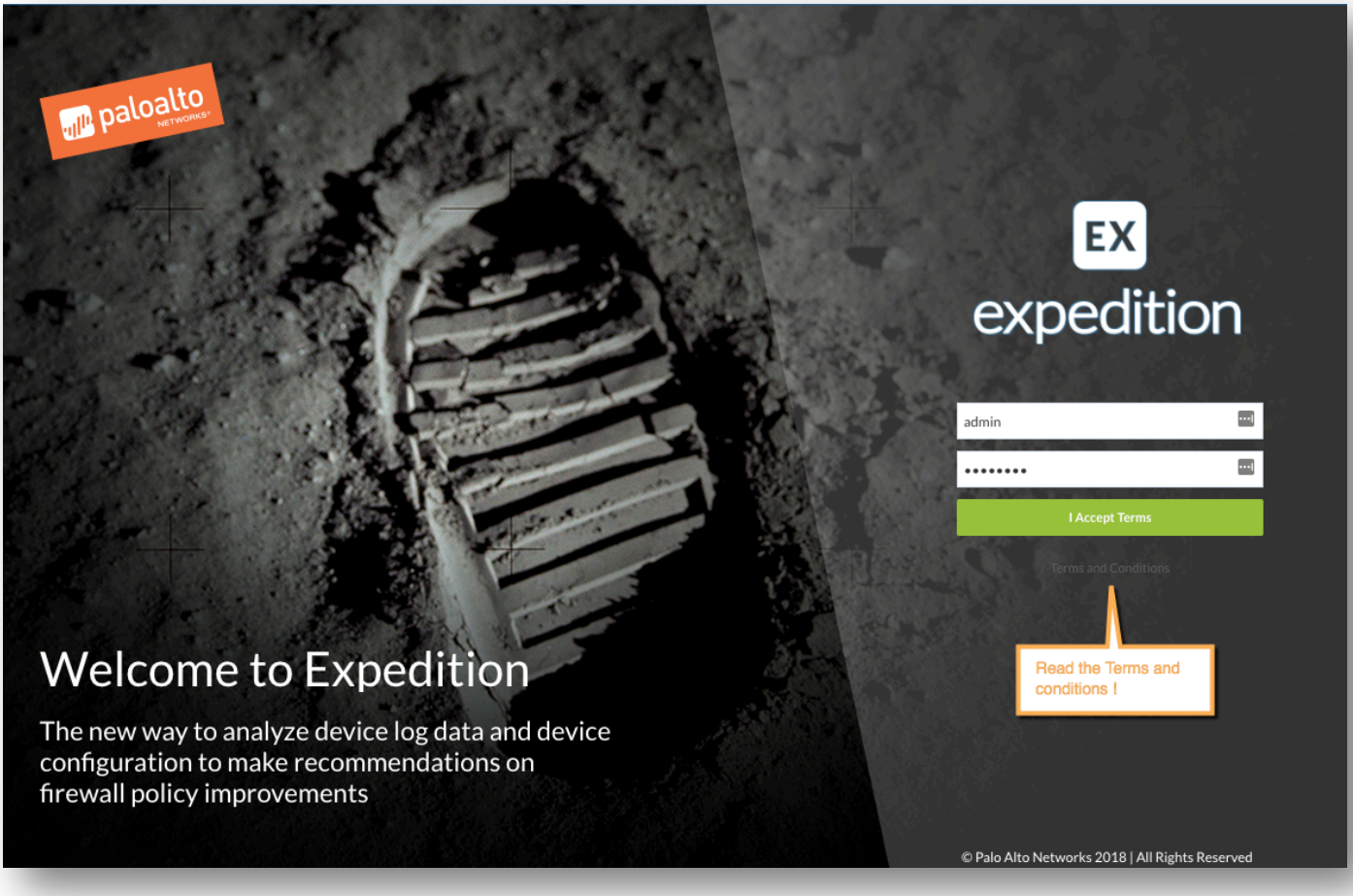
Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The main purpose of this tool was help reducing the time and efforts to migrate a configuration from one of the supported vendors to Palo Alto Networks.

By using the Migration Tool everyone can convert a configuration from Checkpoint or Cisco or any other vendor to a PanOS and give you more time to improve the results. Migration Tool 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well.

With Expedition we have gone one step further, not only because we want to continue helping to facilitate the transition of a security policy from others vendors to PanOS but we want to ensure the outcome it's the best as possible, there is why we added a **Machine Learning module** who can help you to generate new security policies based on real log traffic and the introduction of the **Best Practices Assessment Tool** to check the configuration complies with the Best Practices recommended by our security experts.

With all these huge improvements we expect the next time you use Expedition the journey to the excellence will be easier.

Login



First time login

When login for the first time into Expedition you will be asked for credentials to login from the GUI or from Console.

Expedition has been shipped with the following usernames and password, they are different so use the right one based on where you are (GUI or CLI).

CLI Login

CLI is referencing when you want to get access through Hipervisor console or via SSH.

Username	expedition
Password	paloalto

GUI Login

GUI it's only referencing the access via web interface

Username	admin
Password	paloalto

Security Warning! We encourage to change them after the first login.

Changing default credentials

As a good practice we recommend you to change the default credentials as soon as you can.

CLI Login

After login via SSH or Hypervisor console:

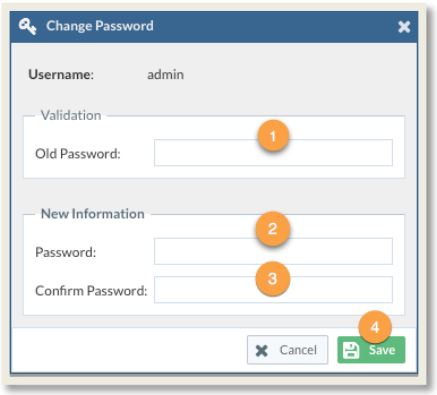
```
# passwd
```

You will be asked to type the current password and then type your new password twice, try to follow some of the recommendations publicly available like this one from SANS Institute:

https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

GUI Login

After login via web browser follow these instructions to change the password for the "admin" user.



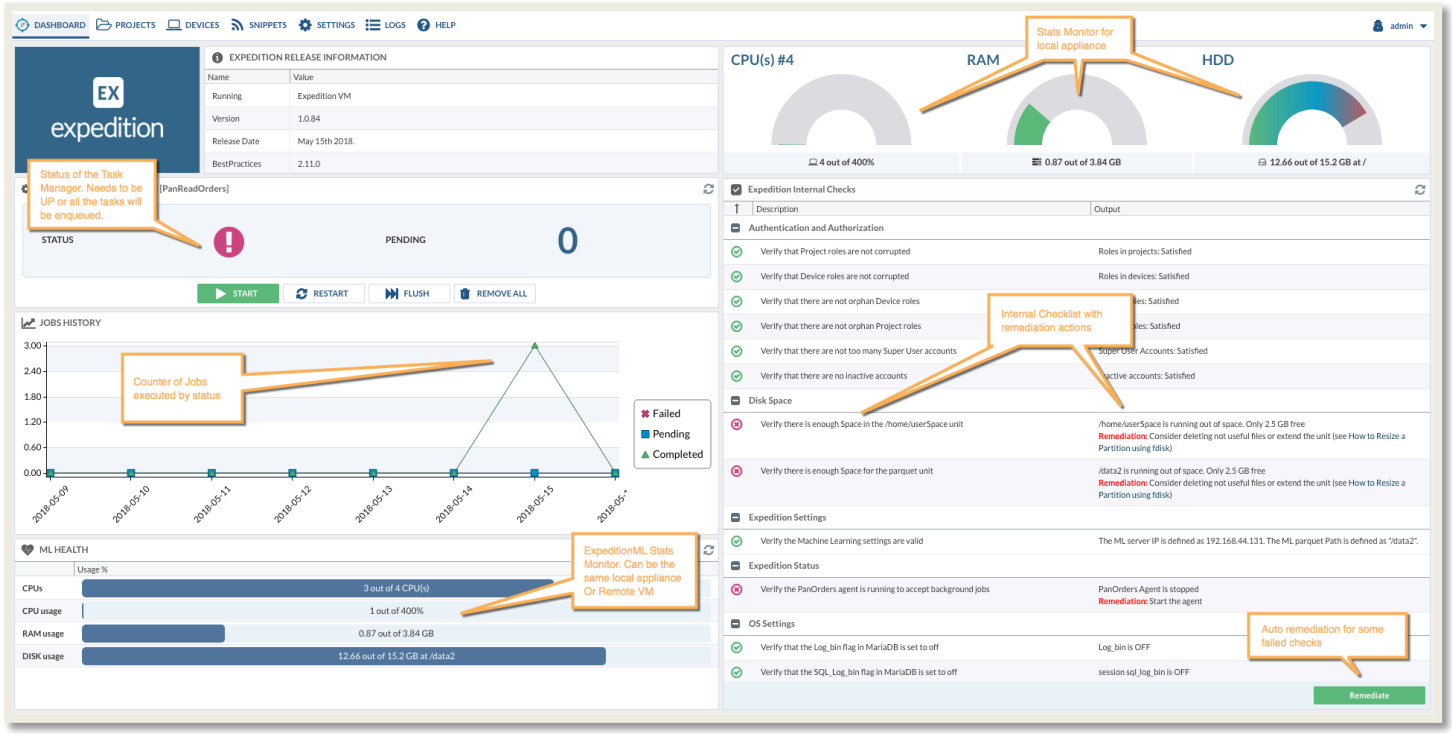
A new window to change the password will be shown:

1. Type the current password
2. Type NEW password
3. Re-type NEW password
4. Click on Save

Remember the password length will be at least 10 characters long

Main Screen

DASHBOARD



Let's walkthrough the Dashboard items:

a) Located at the top-left we can read the current release information and the latest version of the Best Practices Assessment tool installed.

b) Under the release information we find the Task Manager information and the status. It's important to keep it started otherwise some of the tasks we will want to run will be queued until gets started. You can track from here how many jobs still in pending state.

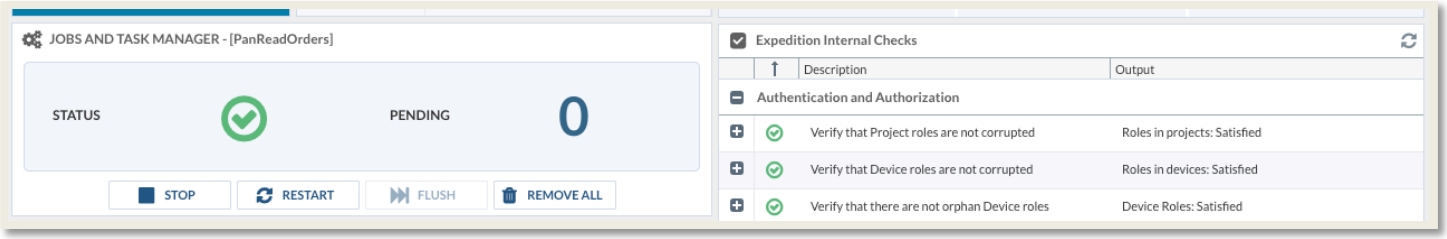
c) Jobs History will chart the output from the tasks executed and how they finished (Failed, Pending, Completed) The chart will show the information related only the last 7 days including the current day.

d) ML Health. This module will track the system status on the Expedition instance running the ML (Machine learning) and data analysis. Usually it's the same device where it runs the GUI and the database but can be an external Expedition instance.

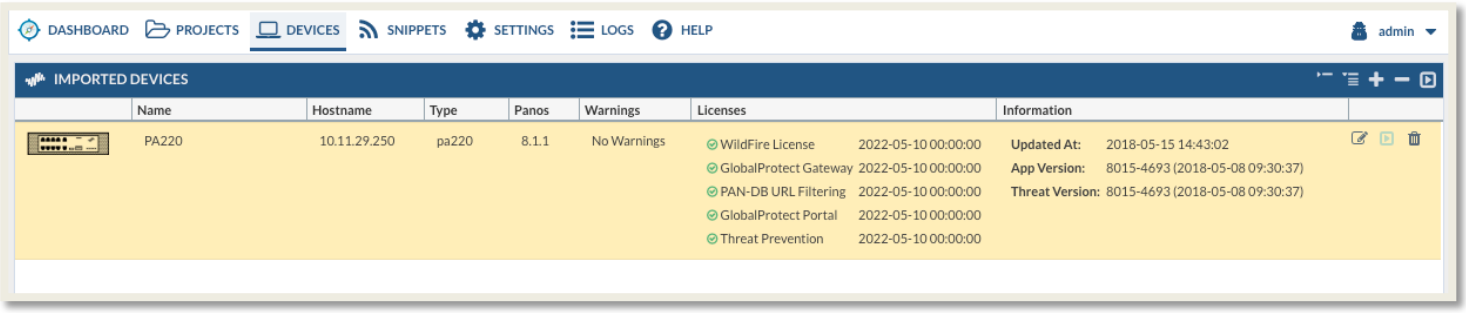
e) Located at the top-right we find the Stats for the local Expedition instance. This shows how the system is doing and consuming the system resources like CPU, RAM and HDD.

f) Below we have a list of internal checks for self-checking. Expedition is tracking for some pieces needed to guarantee the perfect function of the instance, like if we have wrong parameters configured for the data analysis or if we are missing some software dependencies. By using the Remediate button Expedition can automatically remediate some of them.

Important Reminder: Keep the Task Manager always UP. In case was down please click on the *START* button and ensure you see the green icon next to the STATUS like in the following screenshot.



DEVICES



You can import your current Palo Alto Networks firewalls and Panorama to Expedition and use them as Base configuration for migrations or just use them to make improvements in your current configuration like by applying best practices or following the recommendations made by the Machine Learning module.

Importing a Next-gen Firewall

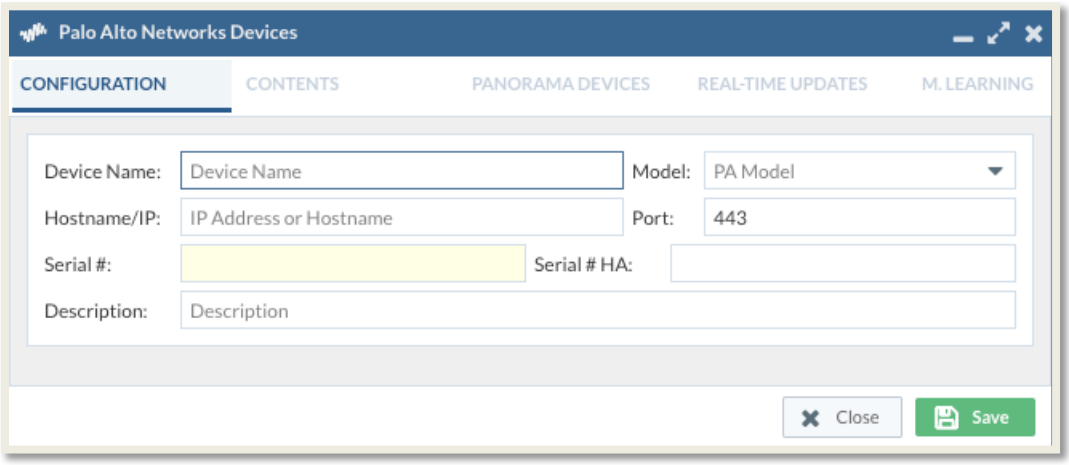
Expedition supports all the PanOS versions since version 4.0 up to 8.1. Let's follow an example on how to create a new Device and import the configuration and securely store it on Expedition.

a) Navigate to the DEVICES tab
b) Add a new Device by clicking on the *plus* button located on the top-right from the panel.

c) A new window will be shown to fill with all the information required.
- Device Name: It's the name you want to call your firewall
- Model: Palo Alto Networks device model
- Hostname/IP: IP or name used to connect to your firewall, if it's a name Expedition needs to know how to resolv it, check the DNS used by Expedition its the right one. You can check from the CLI

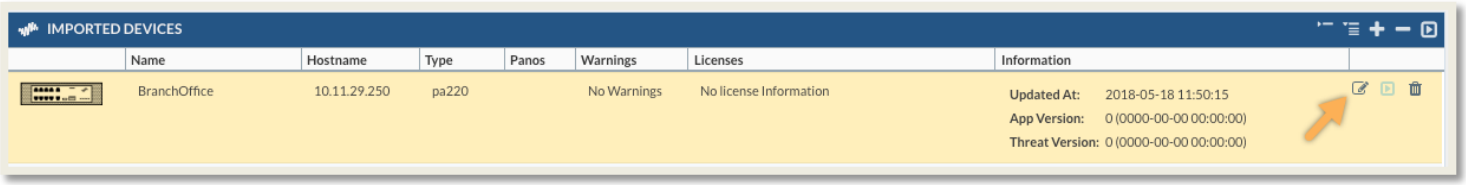
```
# sudo cat /etc/resolv.conf
```

- Port: where the management is running, by default 443
- Serial #: This field is required and will be used as Index to use the right one.
- Serial # HA: In case this firewall is part of a Cluster you can set the HA serial. This will matter for the Machine Learning module which will be explained in another chapter of this document.



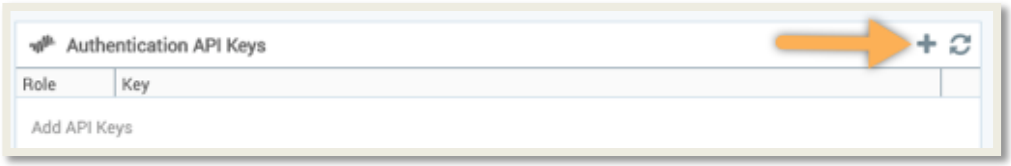
- Click on Save to add the Device to Expedition

d) Once the Device has been created and listed from the Devices view we have to edit add it the credentials to retrieve the contents like applications database, system information and the configuration. Select the device and double click to edit it or by clicking on the Edit button (pencil).

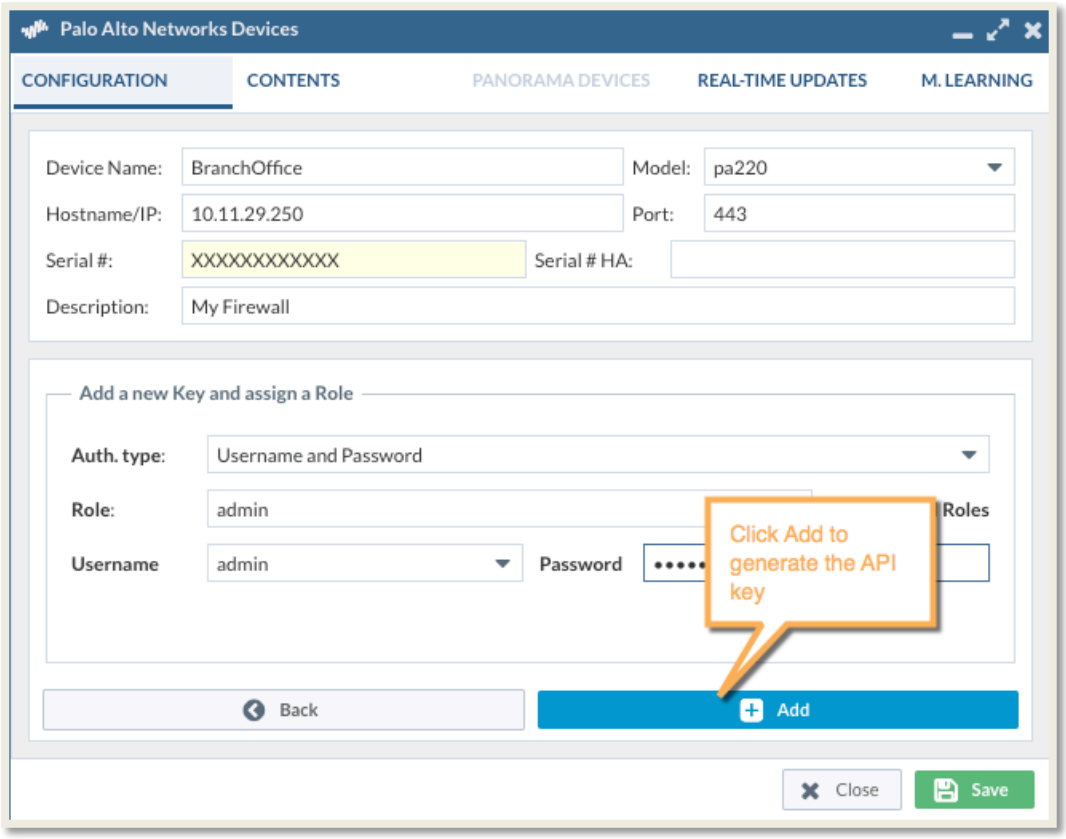


e) The Edit Device window now is displayed. From the Configuration Tab let's add our credentials to connect to the firewall and Expedition will request to the firewall to generate a new API key.
notice the generated API Key will be valid as long as the user don't change the password from the firewall.

- Click on the plus icon to add a new API Keys



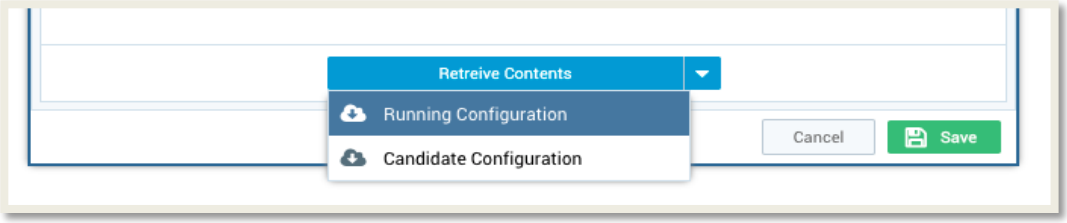
- Auth. Type: How we want to authenticate against he firewalls, we can choose to provide username and password and let Expedition request the API key to your firewall or in case you already have the API key choose API KEY and paste your key in the text field

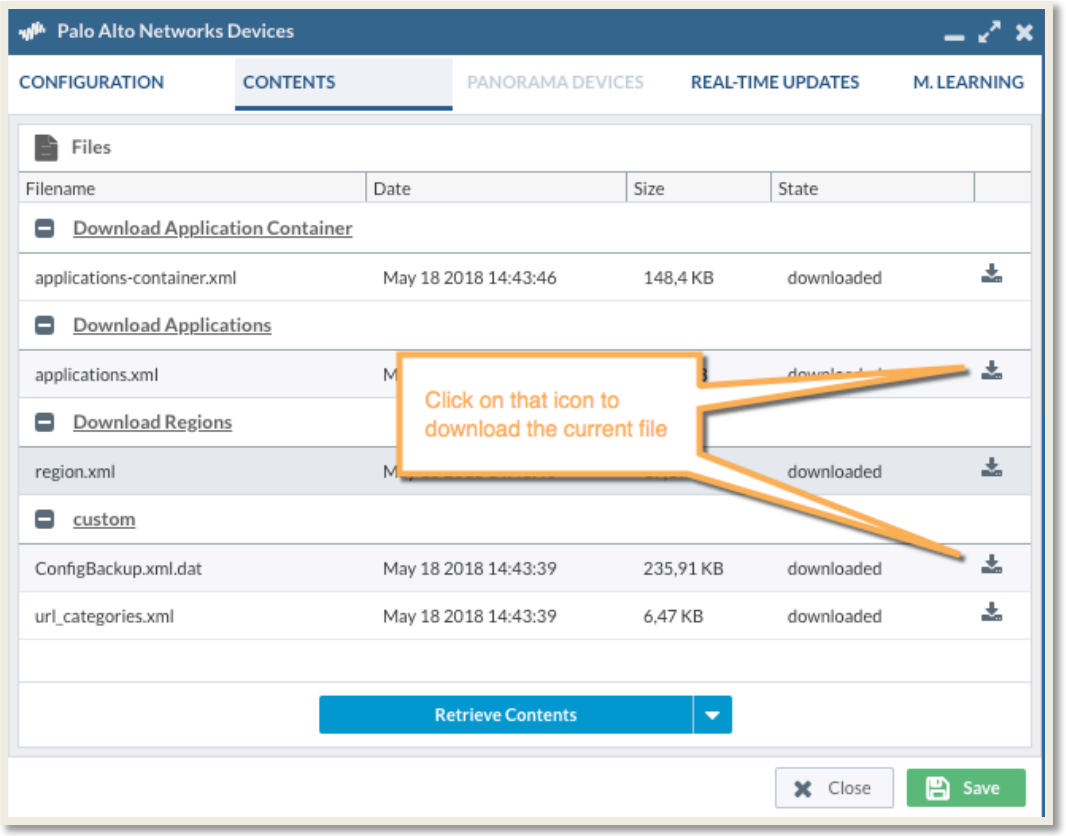


In this example we are going to use Username and Password and provide them

- Role and Apply all Roles: When you add a new API Key this can be attached to a Role inside Expedition, that means when you have a user from Expedition with Role admin inside one Project and that user tries to push changes using API Keys Expedition will use the API Key based on the user's Role in this example admin. If you didn't add an API key to the admin role that user will be unable to send any API Call out. For small environments where you will have only one user and it will be admin there is no need to check the Apply all Roles and keep that key only attached to the admin Role.
- Click on the Add blue button to generate the Keys.

- Navigate to CONTENTS to retrieve the Running configuration.





- Click on *Save* after the downloading process finishes.

Expedition downloaded the device configuration and stored in the hard-drive encrypted. You can check the file from the CLI by entering in the following folder:

```
$ cd /home/userSpace
$ cd  devices
$ cd <the device serial number >
$ ls -la
```

For debugging purposes there is a file on the devices folder called “debug.txt”. The content of this file comes from the daemon who controls the access to the firewalls so expect to find the API requests made to retrieve the keys or dynamic reports in some cases, for security we stripped out the parameter key from the request. So, in case you want to re-use an API call you will have to add at the end the &key=<and your API key>

At this moment Expedition keeps a snapshot of your running configuration. In case you make any change on the device and you want to update your snapshot you have to edit the Device again and retrieve the running configuration again.

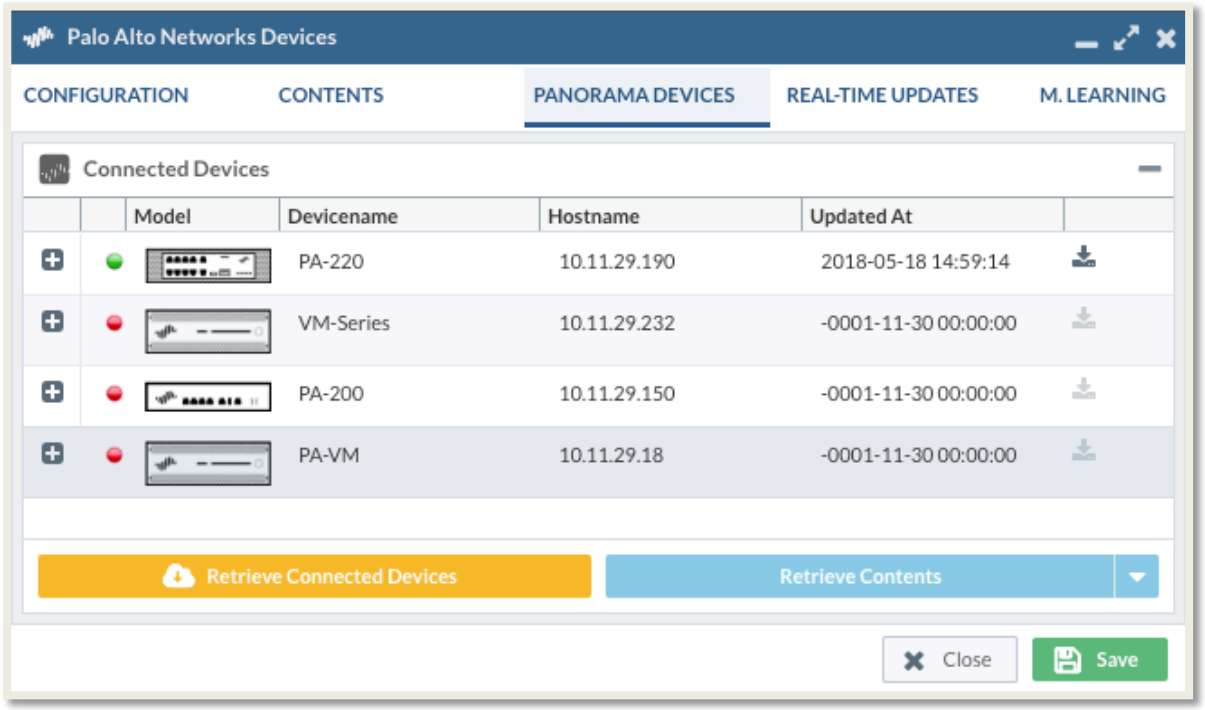
If you were already using that config on a project and you want to import the changes there is no other way than remove the current config from the project and import the device config again, all changes you made on that config and not exported will be lost.

Importing Panorama

Importing a Panorama is really similar to import a Next-gen Firewall and here we will show only what's is different

You can do same steps used to create a new Next-gen Firewall, generate the API keys and retrieve the Contents, now a new tab called PANORAMA DEVICES will be active, so click on that tab.

1. If we need to play with the firewalls connected to that Panorama we need to know them first, so click on Retrieve Connected Devices. This will request that information to Panorama and create the devices on Expedition but referencing them under this Panorama device. That means all the requests we will generate to talk with that Firewall will be done using Panorama as a Proxy.

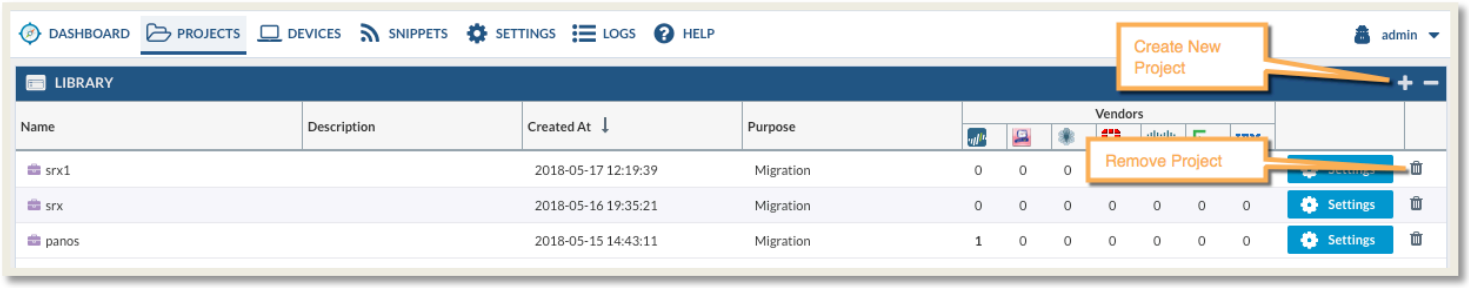


2. In case we need to download the configuration of one of these devices just select it from the list and click on Retrieve Contents. This will allow you to import the configuration of that firewall into your project once we create the project.

If you have one firewall created in Expedition and then you import Panorama and the that firewall its listed as one of the connected devices to that panorama (Serial Number is used as index here) the existing firewall in Expedition will go under the Panorama management meaning from that moment the API requests against it will pass through Panorama.

From the Devices view we can hide all the connected devices to its Panorama by using the following buttons from the Panel header

PROJECTS

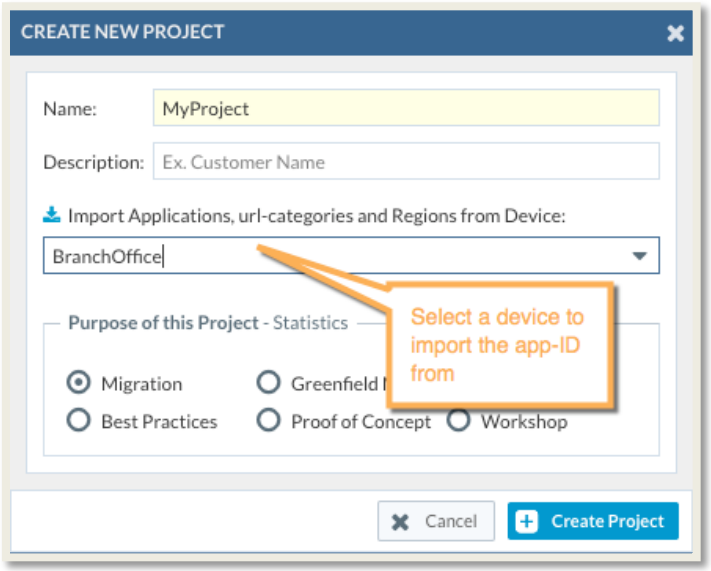


Create a Project

In Expedition each project has its own database. You can create as much projects as you want.

Let's create a new project and see the workflow we have to follow:

a) Click on the plus button to create a new Project
b) A new window will pop up, assign a name to your Project and in case you already created a Device you can select it from the combo box, when you select a firewall or panorama on that combo box you are forcing Expedition to import the same Applications database to your project, that Applications database was downloaded to Expedition at the same time we were retrieving the configuration. Doing this your Project will have the same applications that your Firewall.
c) Purpose if this Project: this is used to provide some statistics but doesn't affect in nothing
d) Click on *Create Project*.

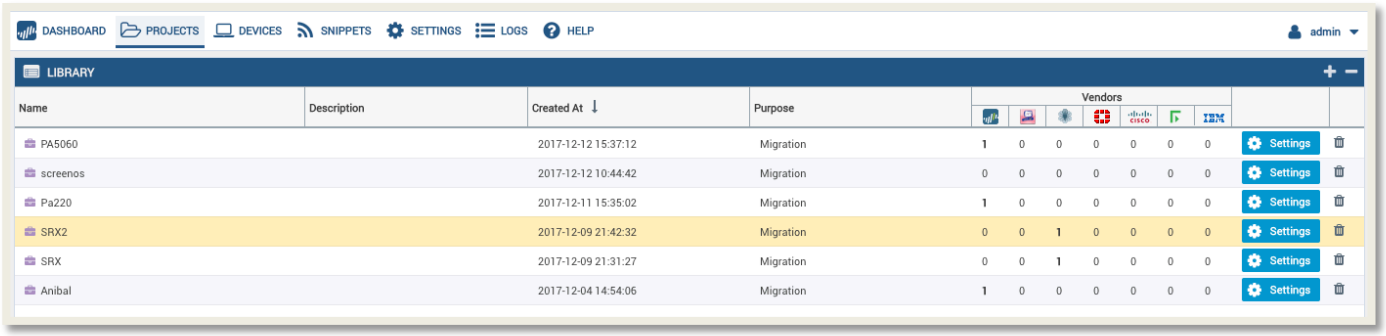


In case we selected a device this will automatically added to your project, you can edit this settings to manage users and devices from within the Project.

Project Settings

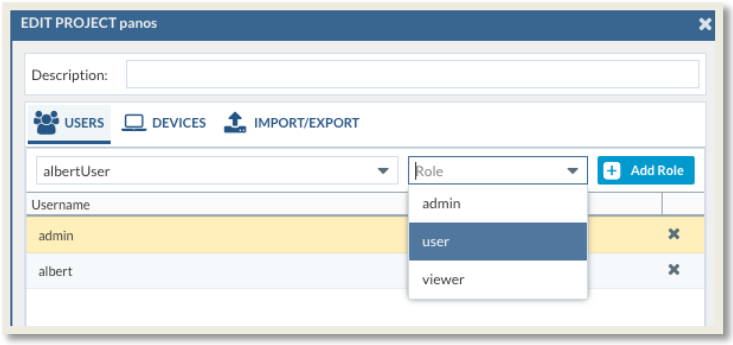
After the project creation we can continue managing the project , we can add more users or devices to the project and import or export the project to be shared with other Expedition instances.

To Edit the Settings just select the Project and click on Settings



Manage Users

We can add more users to a project and attach a Role that the user will have inside the Project.



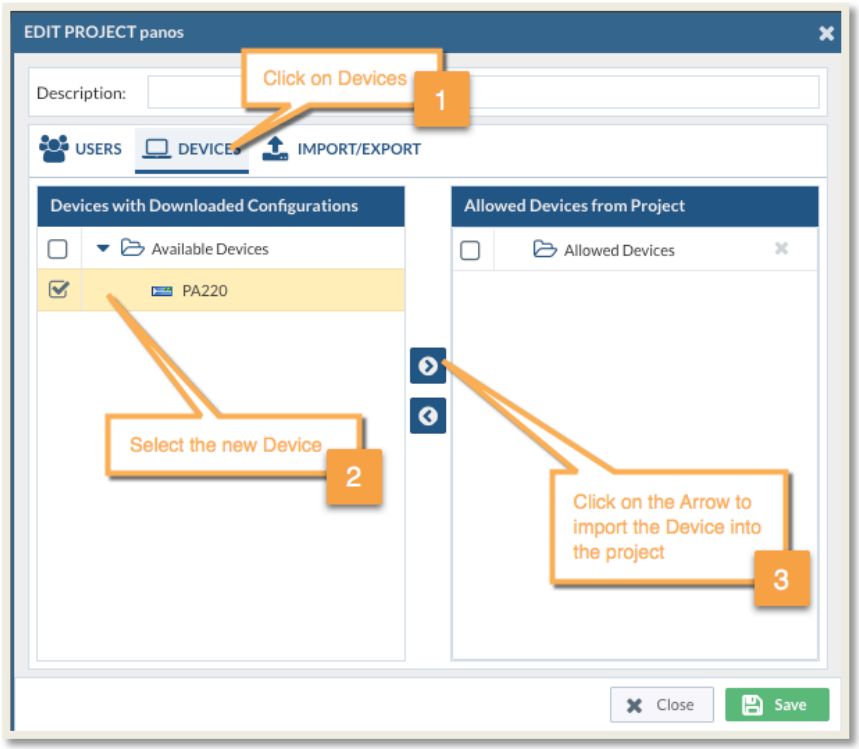
There are 3 Role types inside a Project:

- Admin: This Role can change the Project Settings and modify all the content within it.
- User: This Role can edit the project contents but it cannot change the project settings to add more devices or users to the project.
- Viewer: This Role is for read-only purposes. Doesn't have any privileges to change nothing inside the project or manage the project settings.

Manage Devices

If we want to allow access to import a configuration from an existing device or enable the users to generate API calls to be send to the device you must allow the project to have access to that device.

To do it just click on Devices and select the firewalls you want to allow and move them to the right panel



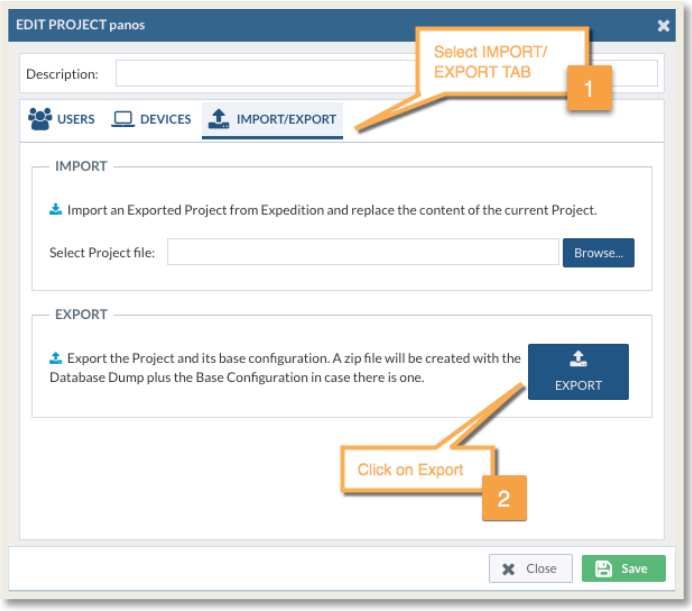
IMPORT / EXPORT

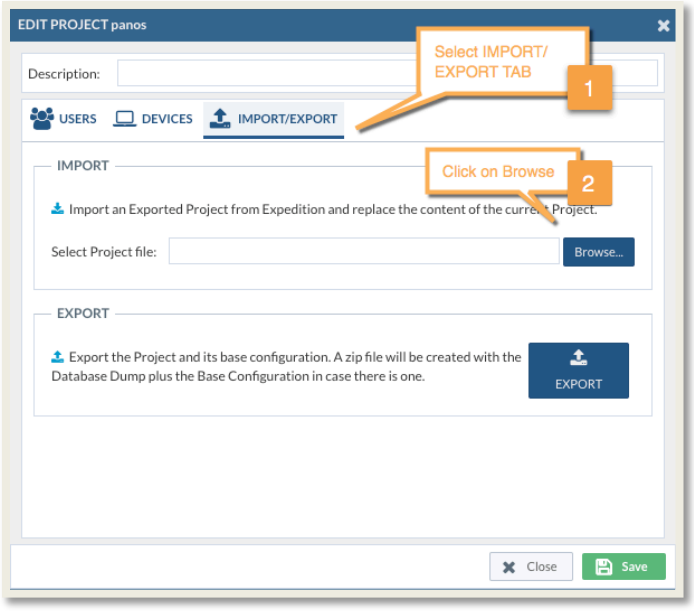
From the tab IMPORT/EXPORT we can export and import the current Project, useful when you want to have a full backup out from Expedition or import it into another instance.

Import a Project: To Import a project you have to create a new Project, assign a NAME and click on Setting to Edit it, after that go to IMPORT/EXPORT and select the file from your desktop.

In case you re-use an existing project the whole content will be overwritten by the imported project

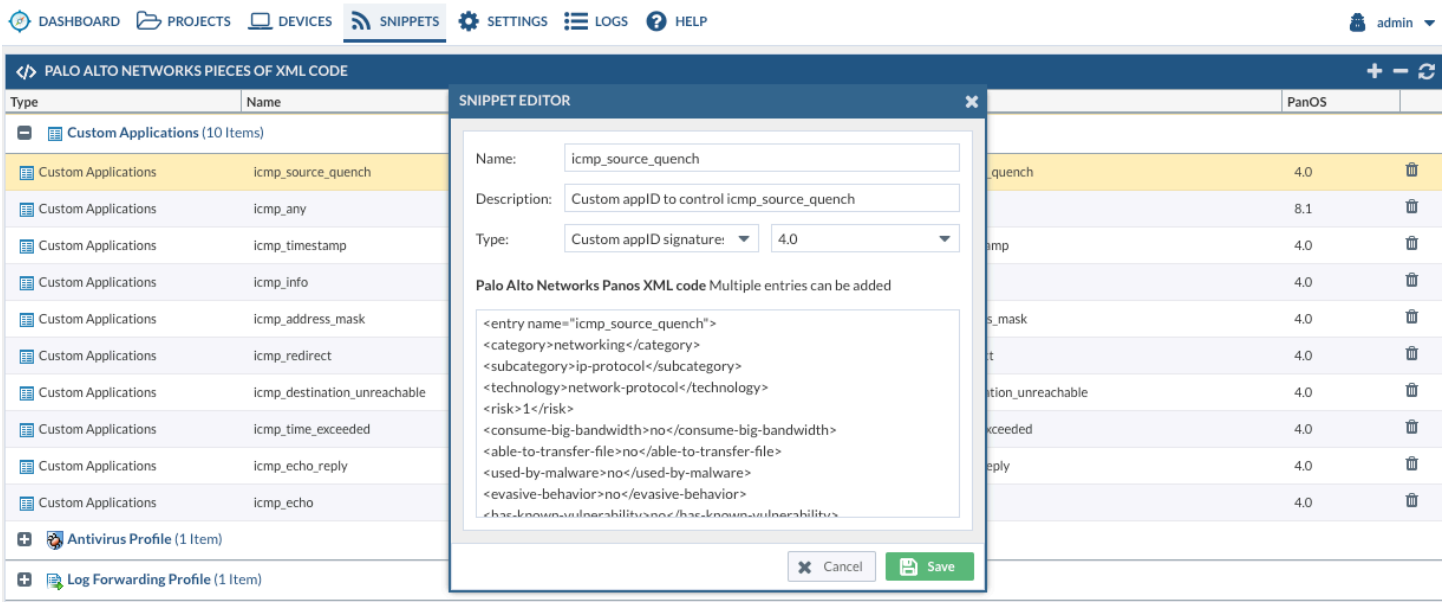
Export a Project: Just Click on EXPORT and save it in your Desktop.





SNIPPETS

Snippets are XML elements from a PanOS configuration, like custom applications or reports, pieces of XML code that can be imported in your projects to be used more than once. If you always use the same type of security profiles and you have migrate configurations form other vendors to Palo Alto Networks quite often then you can write them down once and import in all the projects you want without having to create them every time.



If you add a new Snippet please verify the content is added and its correct, the recommendation is open a XML PanOS file and just copy and paste the content wanted to avoid mistakes. Never leave a Snippet with the content empty, this will prevent Expedition to generate the configuration at the end of your migration.

The Snippets are a global concept only can be added from here and are available from all the Projects.

SETTINGS

Expedition introduces a new Role-based access control system integrated, this allow us to have multiple users with different roles and the possibility to delegate the authentication to external servers like LDAP or RADIUS.

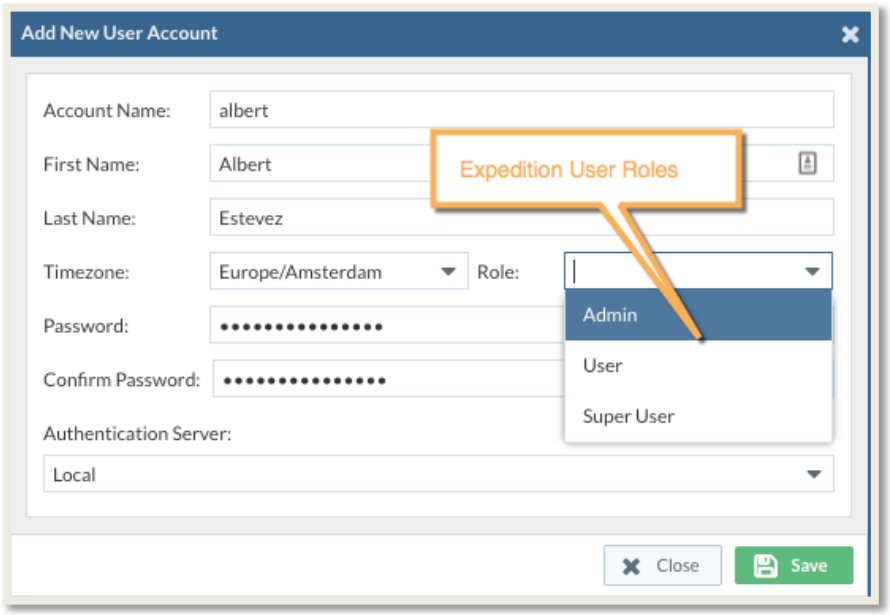
USERS

Create as many users as you need. At least one Super-User is required to Manage Expedition, from there you can create more admin users or read-only users.

The roles available are:

- Super User: This Role allows the User to manage everything on Expedition
- Admin: This Role allows the user to Create projects and devices but cannot change system settings or add new users
- User: This Role allows the user only to enter on Expedition and see projects and devices where has been granted access.

Example on how to create a new User: Click on the plus button.



Select a unique name for the Account Name, choose the Role you want to give to that user and select Local for the Authentication Server in case the authentication is provided by Expedition, if not choose your LDAP or RADIUS profile previously defined.

Revision History

Date	Revision	Comment
May 28, 2018	A	First release of this document.