Palo Alto Networks Firewall Initial Configuration

Tech Note

PAN-OS 4.1

Revision A

Contents

Overview

Congratulations on purchasing a Palo Alto Networks firewall! This document will walk you through the steps to install, register, and license your firewall so that you can begin creating your security policies.

Requirements

Before you begin, locate the email you received from orders@paloaltonetworks.com with the subject "Order Confirmation for Palo Alto Networks order *order_numb*er. This email contains the authorization codes you will need to activate the subscriptions you purchased. If you cannot locate the email, contact support (https://support.paloaltonetworks.com) or ask your Sales Engineer for your activation codes.

Part 1: Configuring the Management Port

Before you can start configuring the security policies that will govern network access throughout your organization, you must set up the management interface (MGT) to enable access via the web interface.

1. Power on the Palo Alto Networks firewall.

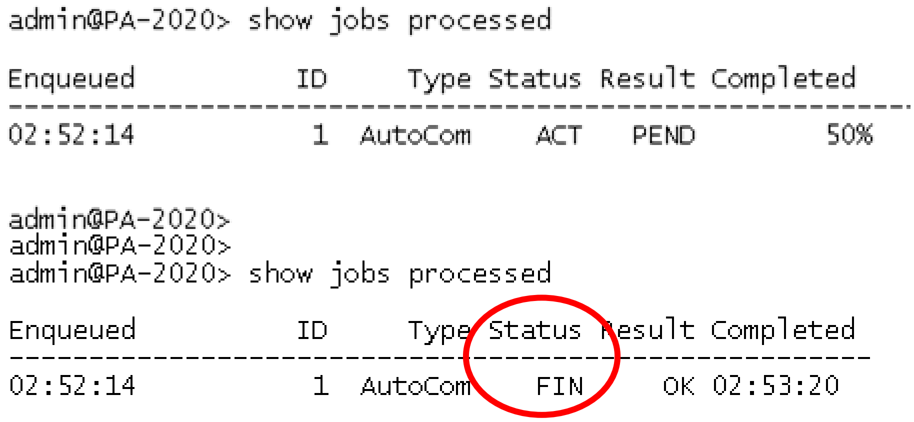
2. Connect a serial cable from your computer to the Console port and connect to the device using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete. The device is not ready for login until the prompt changes to the name of the device, for example: "PA-500 login:".

   Note: *You can also access the device by connecting an RJ-45 Ethernet cable from your computer to the MGT port on the device. You can then launch a browser and go to the following URL: https://192.168.1.1. Note that you may need to change the IP address on your computer to an address in the 192.168.1.0 network, such as 192.168.1.2, in order to access this URL.*

3. Log in using the defaults:

   Username: **admin**
   Password: **admin**

4. You will receive a message that the system is initializing. It may take a few minutes for the device to initialize. You can monitor the status of the startup using the CLI command **show jobs processed**. When the output of this command shows a status of FIN, the configuration is fully loaded and ready for operation.



```
admin@PA-2020> show jobs processed

Enqueued          ID     Type Status Result Completed
---------------------------------------------------------
02:52:14           1  AutoCom    ACT    PEND        50%


admin@PA-2020>
admin@PA-2020>
admin@PA-2020> show jobs processed

Enqueued          ID     Type Status Result Completed
------------------------------------------------------
02:52:14           1  AutoCom    FIN      OK 02:53:20
```

Do not proceed until the device has completely initialized.

5. You will now configure the management interface of the Palo Alto Networks firewall. Fill in the following information:

   MGT interface IP: ______________________

   MGT interface mask: ____________________

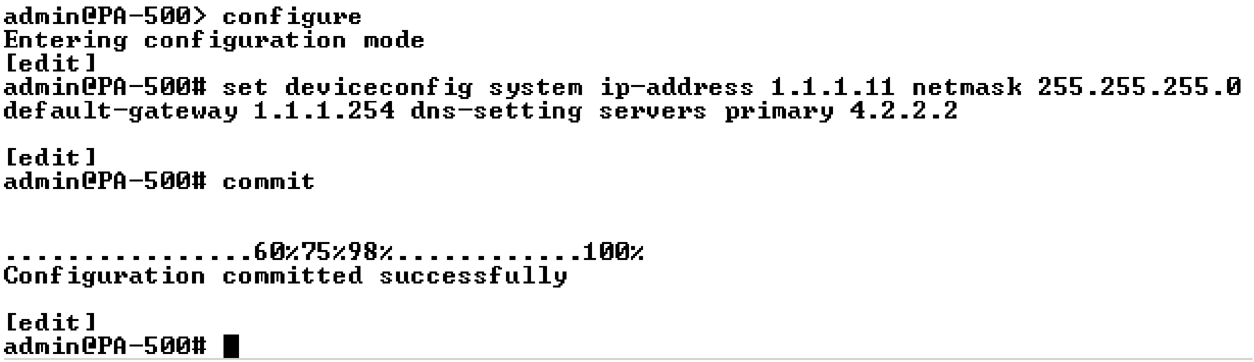
   MGT interface gateway: __________________

   MGT interface DNS server: _______________

6. From the console, run the following commands, making sure to replace the variables with the information you recorded in the previous step:

   configure
   set deviceconfig system ip-address *x.x.x.x* netmask *y.y.y.y* default-gateway *z.z.z.z* dns-setting servers primary *v.v.v.v*
   commit
   exit

   Here is an example of these commands:



```
admin@PA-500> configure
Entering configuration mode
[edit]
admin@PA-500# set deviceconfig system ip-address 1.1.1.11 netmask 255.255.255.0
default-gateway 1.1.1.254 dns-setting servers primary 4.2.2.2

[edit]
admin@PA-500# commit


.................60%75%98%.............100%
Configuration committed successfully

[edit]
admin@PA-500# █
```

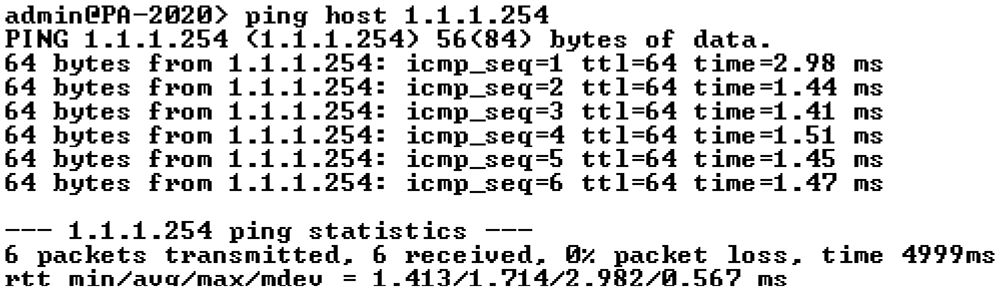
7. Connect the firewall’s management port to your network. The management port must be cabled to a switch port that is set to **auto-detect all settings**.

8. To test connectivity, ping from the firewall to a device on your network, for example, ping to your default gateway (z.z.z.z)

   ping host *hostname or ip_address*

   Press control-C to end the pings.

Here is an example:



```
admin@PA-2020> ping host 1.1.1.254
PING 1.1.1.254 (1.1.1.254) 56(84) bytes of data.
64 bytes from 1.1.1.254: icmp_seq=1 ttl=64 time=2.98 ms
64 bytes from 1.1.1.254: icmp_seq=2 ttl=64 time=1.44 ms
64 bytes from 1.1.1.254: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 1.1.1.254: icmp_seq=4 ttl=64 time=1.51 ms
64 bytes from 1.1.1.254: icmp_seq=5 ttl=64 time=1.45 ms
64 bytes from 1.1.1.254: icmp_seq=6 ttl=64 time=1.47 ms

--- 1.1.1.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 1.413/1.714/2.982/0.567 ms
```

You should test network connectivity to the DNS server, as well as to the Internet.

Note: The firewall must have Internet access so that it can download licenses and the latest version of PAN-OS. You should also ping the server from which you will download licenses and updates: updates.paloaltonetworks.com.

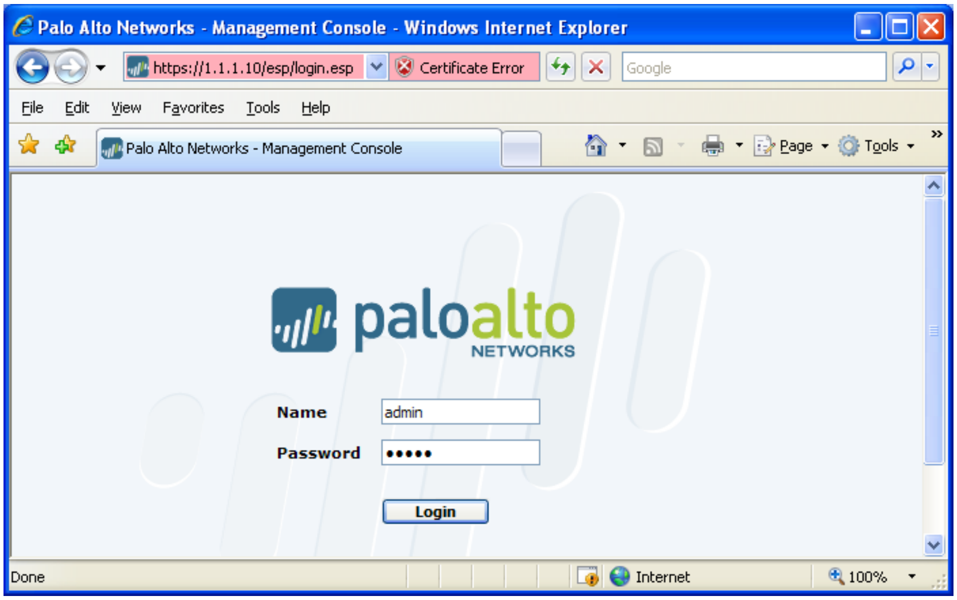
```
admin@PA-200> ping host updates.paloaltonetworks.com
PING updates.paloaltonetworks.com (67.192.236.252) 56(84) bytes of data.
64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=40.5 ms
64 bytes from 67.192.236.252: icmp_seq=2 ttl=243 time=53.6 ms
64 bytes from 67.192.236.252: icmp_seq=3 ttl=243 time=79.6 ms
^C
```

Do not proceed until you have the proper connectivity.

Part 2: Installing Licenses and Updating Software

You will use the web interface of the firewall for the remainder of the configuration.

1. On the management workstation, open a browser to the IP address you just assigned to your management interface. Make sure to use SSL to connect to the firewall (https://<IP_address>). You will see a certificate warning—that is ok; continue to the web page. You will be prompted with a login screen.



Palo Alto Networks - Management Console - Windows Internet Explorer

https://1.1.1.10/esp/login.esp

Certificate Error

Name: admin

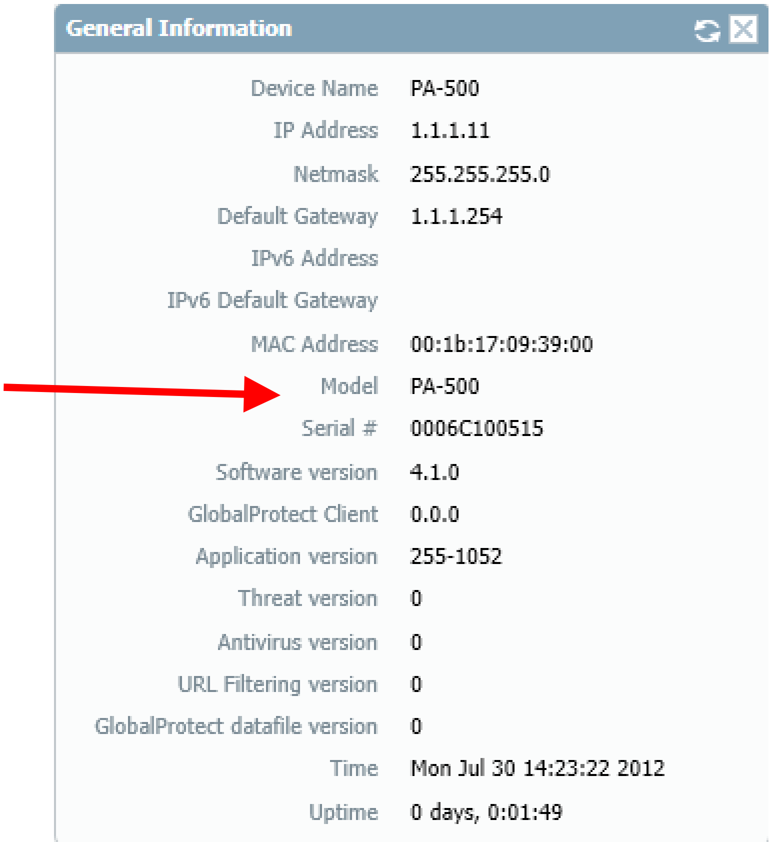
Password: •••••

2. Log in to the firewall with the same username and password that you used to log in to the console during the initial configuration (admin/admin). Upon successful login, the home screen will appear. You will use the tabs across the top, and the menus in the left column, to configure the device.

   Note: *If you have connectivity problems when trying to access the web interface, make sure that the switch port that is physically cabled to the device's management port is set to "auto".*

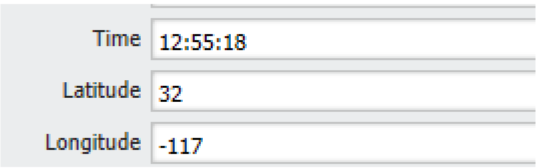
3. Configure a more secure administrator password using **Device** >**Administrators**. Make sure to write down this new password and store it in a safe place.

4. You must register the device before you can download your licenses. Go to https://support.paloaltonetworks.com. Click **Register**. Enter the appropriate information to create a login account and enter the device serial number on that page. You can find your device's serial number in the General Information section of the Dashboard.



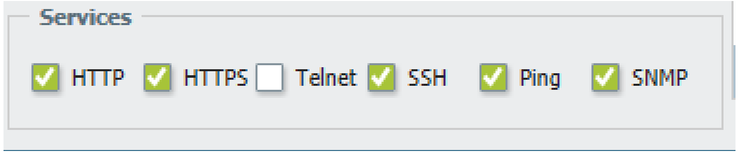
Device Name	PA-500
IP Address	1.1.1.11
Netmask	255.255.255.0
Default Gateway	1.1.1.254
IPv6 Address	
IPv6 Default Gateway	
MAC Address	00:1b:17:09:39:00
Model	PA-500
Serial #	0006C100515
Software version	4.1.0
GlobalProtect Client	0.0.0
Application version	255-1052
Threat version	0
Antivirus version	0
URL Filtering version	0
GlobalProtect datafile version	0
Time	Mon Jul 30 14:23:22 2012
Uptime	0 days, 0:01:49

5. Go to the **Device** > **Setup** -> **Management** tab. In the **General Setting** section, click the Edit (⚙) icon to edit the settings. Enter the current date and time, and the appropriate time zone. You can also enter the latitude and longitude of your location. This will place the graphic for your firewall in the proper location on the world map. The example below is appropriate for San Diego, CA:



Time	12:55:18
Latitude	32
Longitude	-117

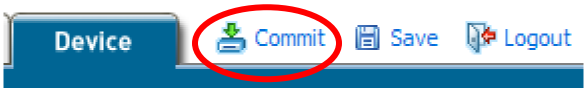
6. On the same screen, edit the Management Interface Settings. Enable the services that you want the MGT interface to respond to:



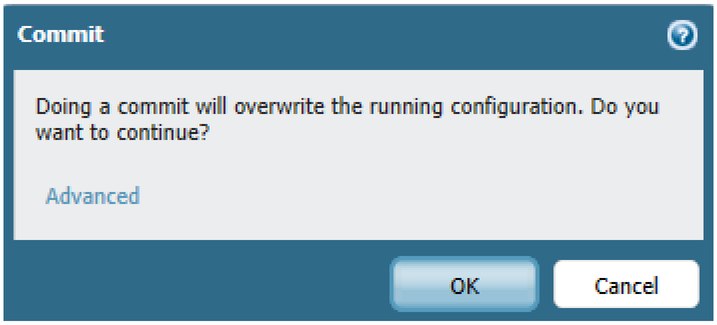
Services

☑ HTTP ☑ HTTPS □ Telnet ☑ SSH ☑ Ping ☑ SNMP

7. To save your configuration settings, click **Commit** in the top-right corner of the browser window.



Confirm your commit.



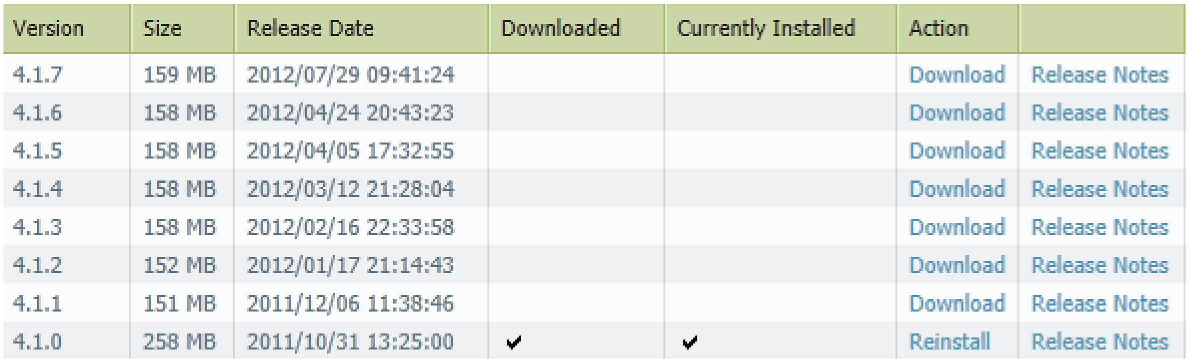
Commit

Doing a commit will overwrite the running configuration. Do you want to continue?

This configuration will be saved to the firewall's hard drive as well as to the running config.

8. Confirm that the device is registered and has access to the update server. Go to **Device** > **Software**. You will see the message "Error: No update information available". At the bottom of the page, click **Check Now**. If you receive an error that the device is not registered, or some other error, you need to troubleshoot connectivity before you proceed.

If there are no errors, a list of the latest versions of PAN-OS will appear:

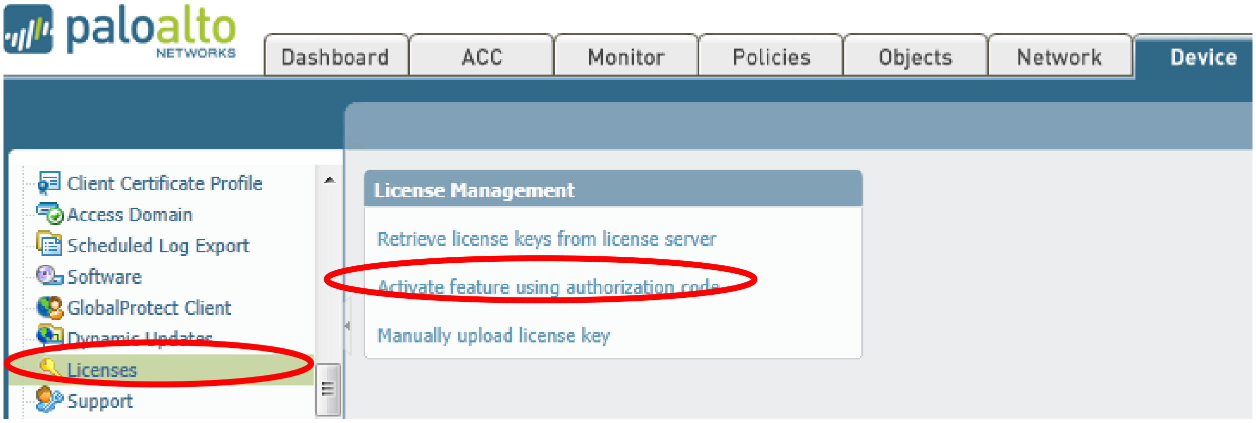


Version	Size	Release Date	Downloaded	Currently Installed	Action	
4.1.7	159 MB	2012/07/29 09:41:24			Download	Release Notes
4.1.6	158 MB	2012/04/24 20:43:23			Download	Release Notes
4.1.5	158 MB	2012/04/05 17:32:55			Download	Release Notes
4.1.4	158 MB	2012/03/12 21:28:04			Download	Release Notes
4.1.3	158 MB	2012/02/16 22:33:58			Download	Release Notes
4.1.2	152 MB	2012/01/17 21:14:43			Download	Release Notes
4.1.1	151 MB	2011/12/06 11:38:46			Download	Release Notes
4.1.0	258 MB	2011/10/31 13:25:00	✓	✓	Reinstall	Release Notes

In this example, PAN-OS 4.1.0 is both downloaded and installed.

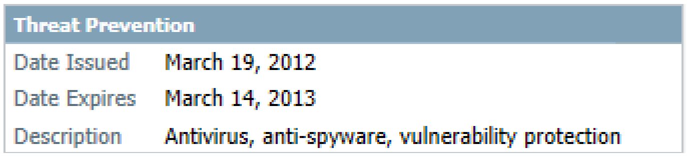
Do not install a new OS just yet; you should retrieve licenses first.

9. You will now activate your licenses. Go to **Device** > **Licenses**. The following screen will appear.



10. Select **Activate feature using authorization code**. Locate the email you received from Palo Alto Networks customer service that lists the subscriptions you purchased, and the associated activation codes. Enter the codes now. After you enter each code, confirm that the license was accepted as follows.

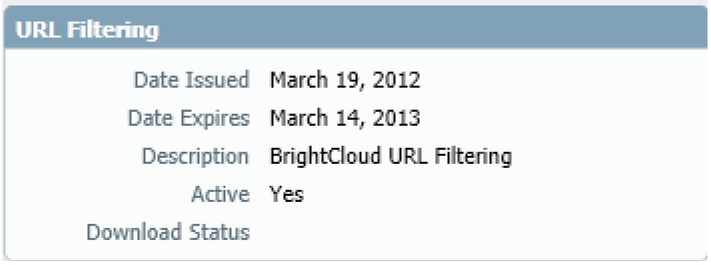
After you enter the threat prevention license, you will see the following on the Licenses page:



Threat Prevention

Date Issued	March 19, 2012
Date Expires	March 14, 2013
Description	Antivirus, anti-spyware, vulnerability protection

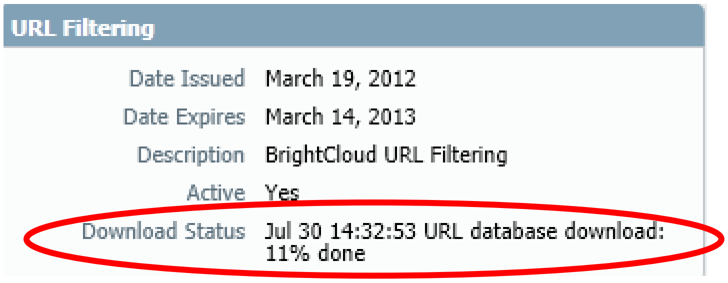
After you enter the URL filtering license, you will see the following on the Licenses page:



URL Filtering

Date Issued	March 19, 2012
Date Expires	March 14, 2013
Description	BrightCloud URL Filtering
Active	Yes
Download Status	

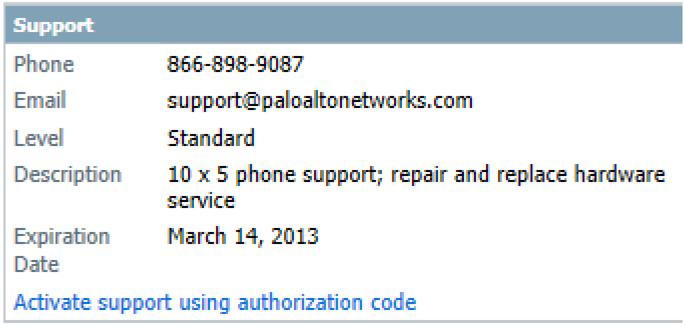
If you refresh the page a minute later, the Download Status will indicate the URL database download has begun:



URL Filtering

Date Issued	March 19, 2012
Date Expires	March 14, 2013
Description	BrightCloud URL Filtering
Active	Yes
Download Status	Jul 30 14:32:53 URL database download: 11% done

After you enter the Support license, you will see the following on the Support page:

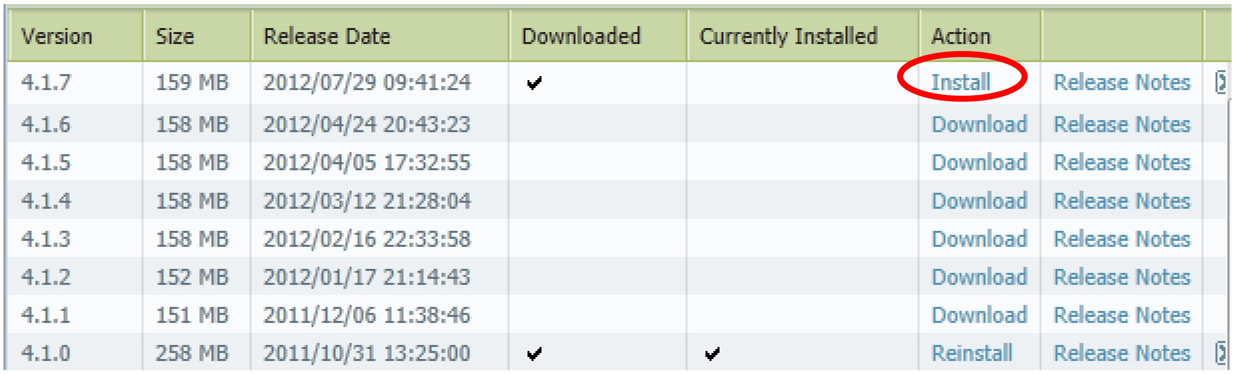


Support	
Phone	866-898-9087
Email	support@paloaltonetworks.com
Level	Standard
Description	10 x 5 phone support; repair and replace hardware service
Expiration Date	March 14, 2013

Activate support using authorization code

Do not proceed until you have successfully entered all the authorization codes for the subscriptions that you have purchased.

11. After you finish activating your subscriptions, you can download and install the latest version of PAN-OS. Select **Device** > **Software** and then select the version of PAN-OS software that your Sales Engineer recommends you install. Click **Download**. After the download completes, you will see a check mark in the Downloaded column and the value in the Action column changes to Install as follows:

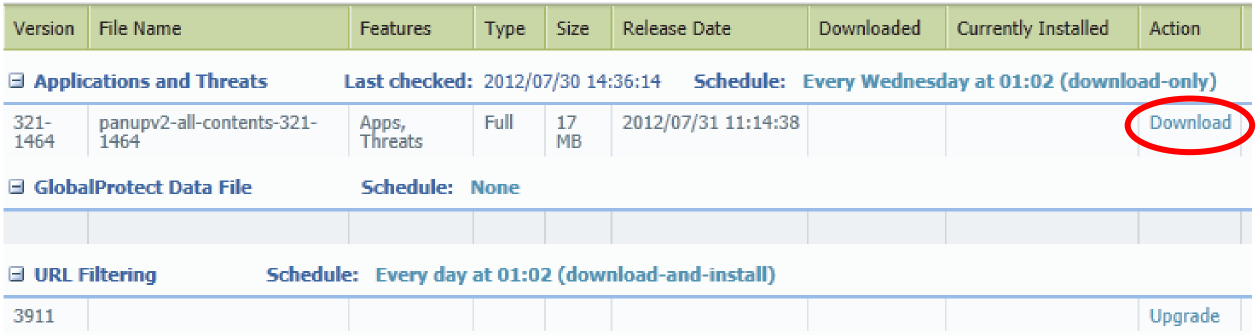


Version	Size	Release Date	Downloaded	Currently Installed	Action	
4.1.7	159 MB	2012/07/29 09:41:24	✓		Install	Release Notes
4.1.6	158 MB	2012/04/24 20:43:23			Download	Release Notes
4.1.5	158 MB	2012/04/05 17:32:55			Download	Release Notes
4.1.4	158 MB	2012/03/12 21:28:04			Download	Release Notes
4.1.3	158 MB	2012/02/16 22:33:58			Download	Release Notes
4.1.2	152 MB	2012/01/17 21:14:43			Download	Release Notes
4.1.1	151 MB	2011/12/06 11:38:46			Download	Release Notes
4.1.0	258 MB	2011/10/31 13:25:00	✓	✓	Reinstall	Release Notes

12. Click **Install** to upgrade the PAN-OS software on the device.

13. When prompted, reboot the device. After the device reboots, log in to the web interface using the new username and password you created.

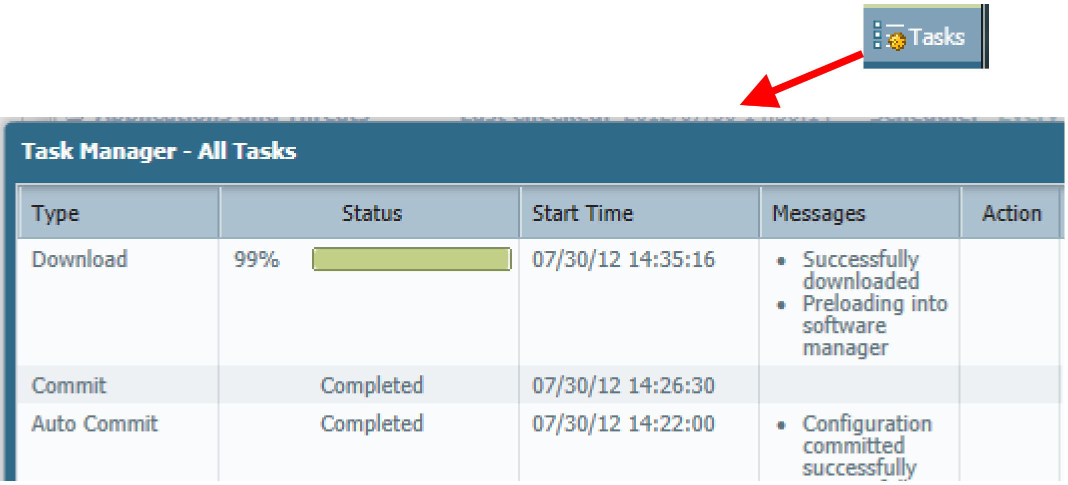
14. To download the latest databases, select **Device** > **Dynamic Updates** and click **Check Now**. You will see an updated list of the various databases. Your screen will look similar to the following:



Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action
⊟ Applications and Threats	Last checked: 2012/07/30 14:36:14	Schedule: Every Wednesday at 01:02 (download-only)						
321-1464	panupv2-all-contents-321-1464	Apps, Threats	Full	17 MB	2012/07/31 11:14:38			Download
⊟ GlobalProtect Data File	Schedule: None							
⊟ URL Filtering	Schedule: Every day at 01:02 (download-and-install)							
3911								Upgrade

Notice that you will not be able to download the AV database until the Application and Threats database is installed.

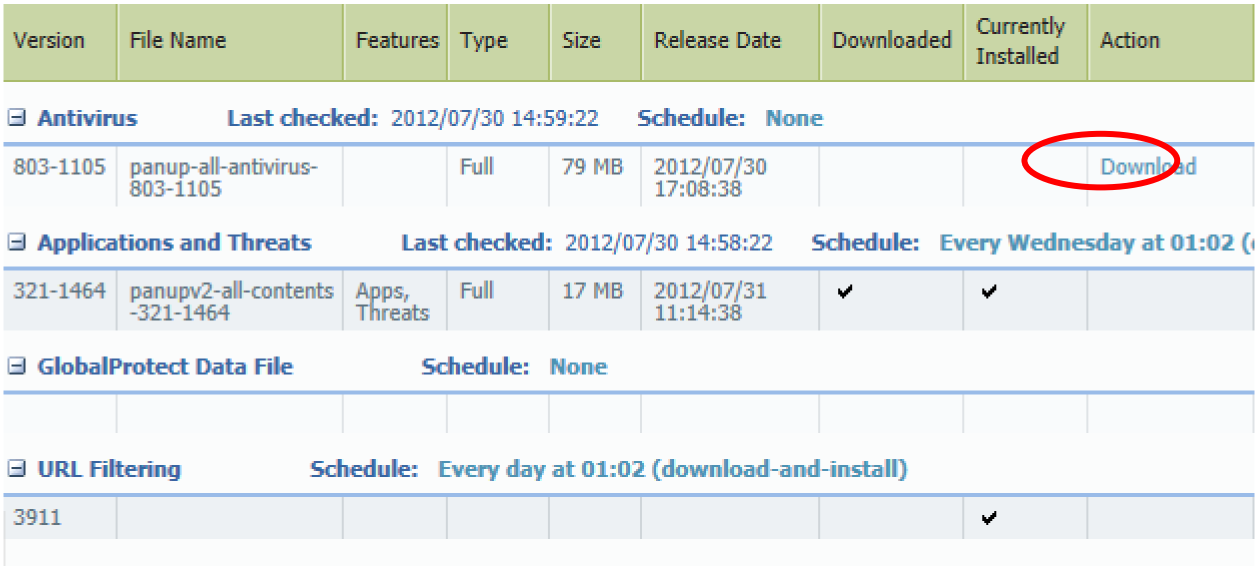
15. **Download** the latest Application and Threats database, and then **Install** it. If you close the download or installation window, you can view the job status using the "Tasks" icon in the bottom right corner of the screen:



Task Manager - All Tasks

Type	Status	Start Time	Messages	Action
Download	99%	07/30/12 14:35:16	• Successfully downloaded • Preloading into software manager	
Commit	Completed	07/30/12 14:26:30		
Auto Commit	Completed	07/30/12 14:22:00	• Configuration committed successfully	

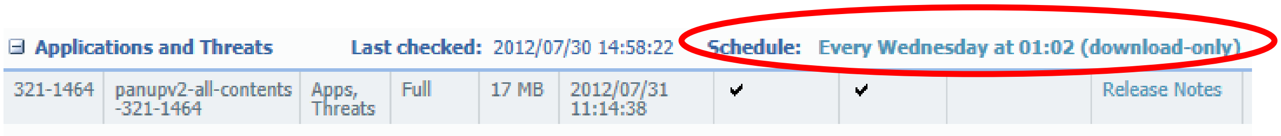
16. While still on the Dynamic Updates screen, click **Check Now**. The latest Antivirus database should now be available for download.



Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action
⊟ **Antivirus**	**Last checked:** 2012/07/30 14:59:22	**Schedule:** None						
803-1105	panup-all-antivirus-803-1105		Full	79 MB	2012/07/30 17:08:38			Download
⊟ **Applications and Threats**	**Last checked:** 2012/07/30 14:58:22	**Schedule:** Every Wednesday at 01:02 (						
321-1464	panupv2-all-contents -321-1464	Apps, Threats	Full	17 MB	2012/07/31 11:14:38	✔	✔	
⊟ **GlobalProtect Data File**	**Schedule:** None							
⊟ **URL Filtering**	**Schedule:** Every day at 01:02 (download-and-install)							
3911							✔	

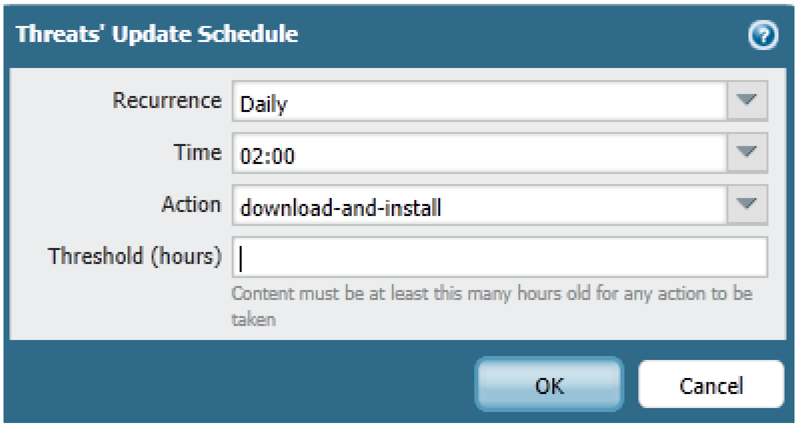
17. **Download** and then **Install** the latest Antivirus database.

18. You will now configure the automatic downloading and installation of the Application database, as well as the AV database. Next to the word "Schedule" for the Applications database, click on the text "Every Wednesday at 01:02 (download-only)" to open the Update Schedule dialog.



⊟ **Applications and Threats**	**Last checked:** 2012/07/30 14:58:22	**Schedule:** Every Wednesday at 01:02 (download-only)							
321-1464	panupv2-all-contents -321-1464	Apps, Threats	Full	17 MB	2012/07/31 11:14:38	✔	✔		Release Notes

19. Configure the update schedule to recur daily, at a time that you select, and configure the database to **download-and-install** automatically.



Threats' Update Schedule

Recurrence: Daily

Time: 02:00

Action: download-and-install

Threshold (hours):

Content must be at least this many hours old for any action to be taken

20. Repeat steps 18 and 19 to automatically download and install the Antivirus database.

21. **Commit** the changes.

Part 3: Firewall Configuration

At this point you can begin configuring the data ports on your firewall and define your zones and security policies. For more information, refer to the following Palo Alto Networks documents:

- PAN-OS Administrator's Guide https://live.paloaltonetworks.com/community/documentation
- PAN-OS Layer 3 Implementation Guide https://live.paloaltonetworks.com/docs/DOC-2561
- PAN-OS Design Guide https://live.paloaltonetworks.com/docs/DOC-2561

Revision History

Date	Revision	Comment
8/1/12	A	First release of this document.