6.2 Migration Notes

https://campus.barracuda.com/doc/71862808/

Before migrating your Barracuda NextGen Firewall F-Series to 6.2.x, review the requirements and changes listed in the following sections. Some changes applied during the migration might require you to make preparations before the update or extra configurations after the update.

Migration path to 6.2.x

You can upgrade to firmware 6.2 from the following firmware versions:

Current Version	Target Version			
	6.2.0	6.2.1	6.2.2	6.2.3
6.0.0 - 6.0.3	Yes	Yes	Yes	Yes
6.0.4	No	Yes	Yes	Yes
6.0.5	No	No	Yes	Yes
6.0.6	No	No	No	Yes
6.0.7	No	No	No	Yes
6.1.0 - 6.1.2	Yes	Yes	Yes	Yes
6.1.3	No	Yes	Yes	Yes

Direct updating from versions 5.x to version 6.2.x is not possible.

For more information, see Migrating from 5.4.x to 6.0.x.

Read the **Release Notes**, especially the **Known Issues** section, for the firmware version that you want to update to.

Review upgrade requirements

Verify that your Barracuda NextGen Firewall F-Series or Barracuda NextGen Control Center meets the upgrade requirements.

Supported models

You can upgrade the following NextGen Firewall F-Series models to 6.2.X:

Barracuda NextGen F-Series and Control Center Models	
Hardware	F10 Rev A/B, F15, F18 Rev A, F80 Rev A, F100 Rev A/B, F101 Rev A/B, F180 Rev A, F200 Rev A/B/C, F201 Rev A/B/C, F280 Rev A/B, F300 Rev A/B, F301 Rev A/B, F380 Rev A , F400 Rev A/B, F600 Rev A/B/C , F800 Rev A/B, F900 Rev A, F1000 Rev A, C 400, C610
Virtual	VF10, VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820
Public Cloud	AWS, Azure
Legacy and Standard Hardware Systems	
Legacy	Legacy phion appliances are not supported for version 6.x or higher.
Standard Hardware	A standard hardware system is a Barracuda NextGen Firewall F-Series running on 3rd-party server hardware using an SF license. Consult the Barracuda Networks Technical Support to find out if your specific standard hardware is supported.

Barracuda NextGen Firewall F10 Rev A

It is not possible to install 6.2.3 via F-Series install / USB stick on a F10 Rev A, due to the low amount of RAM. Install 6.2.1 via F-Series Install and then update to 6.2.3 instead.

Disk space requirements

You must have at least 50 MB of free space in the **/boot/** partition and twice the size of the update package in the **/** (root) partition.

Upgrading a high availability (HA) unit without upgrading its HA partner unit

If you are upgrading a unit in a high availability (HA) cluster without upgrading its partner, you must re-synchronize both units:

1. Go to **FIREWALL > Live > Show Proc**.
2. Select the **Sync Handler** process and select **Kill Selected**.
   The process is automatically restarted after a couple of seconds, and the primary and secondary unit automatically synchronize their sessions.

Barracuda NextGen Admin

After updating a system, you must also download NextGen Admin with the same version. NextGen Admin is backward-compatible. That means you can manage 5.x, and 6.x F-Series Firewalls and Control Centers with NextGen Admin 6.2.1.

> Always use the latest version of Barracuda NextGen Admin.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

As of January 31, 2019, the first-generation ATP cloud services used by default with firmware versions 6.2.x, 7.0.x, 7.1.0, 7.1.1, and 7.2.0 will be discontinued. Firewalls using ATP must switch to the second-generation ATP cloud service, which is known as Barracuda Advanced Threat Protection (BATP).

The following table gives an overview of the options you have when you run a special firmware version:

Product	Your Current Firmware Version	Migrating Option
Stand-alone Box or Manged Box	6.x ... 7.0.x	Firmware 7.0.x is end-of-support in December 2018! Update to the latest 7.1.x or 7.2.x releases, which are using BATP, without the need for further changes. For more information, see **How to Install Updates via NextGen Admin** on *campus.barracuda.com*.

Migration instructions for 6.2.3

When upgrading from 6.0.x or 6.1.X to 6.2.3, you must complete the migration steps for 6.2.0, 6.2.1, and 6.2.3.

Clam AV Pattern Updates

- (legacy licensed firewalls only) The freshclam fallback pattern updates must be enabled manually on all legacy, phion-licensed firewalls to continue receiving update for ClamAV.

Migration instructions for 6.2.2

No manual migration steps required to update to firmware version 6.2.2 from 6.2.1. If you are updating from an earlier version, you must complete the migration steps for 6.2.0 and 6.2.1.

Migration instructions for 6.2.1

When upgrading from 6.0.x or 6.1.X to 6.2.1, you must complete the migration steps for 6.2.0 and 6.2.1.

Secure Web Proxy

- The Secure Web Proxy is no longer supported with firmware version 6.2.1. Remove the service before updating to 6.2.1. Use SSL Interception and URL Filtering in the Firewall or HTTP Proxy instead.
  For more information, see How to Configure SSL Interception in the Firewall, or How to Set Up and Configure the HTTP Proxy.

Barracuda Activation

- To show the correct license expiration date for the subscription licenses, you must delete and download, or otherwise re-import, the licenses. When licenses are renewed, the expiration date is automatically corrected. If you do not re-import the licenses, the expiration of the subscription licenses is not displayed correctly and the base license expiration date is shown instead.

Migration instructions for 6.2.0

When upgrading according to the migration path above, you must complete the migration steps listed below:

Azure UDR Networking

When updating an F-Series Firewall in Azure from 6.1.X to 6.2.0, complete a dummy change in **Box > Network > Azure Networking** and trigger a soft network activation after updating.

Content Matching

Application rules that use the legacy **Content** matching must be removed before updating with NextGen Admin version 6.1.x or 6.0.x. After the update, recreate the application rules using the new File Content Policy Filtering with NextGen Admin 6.2.0.

URL Filter

F-Series Firewalls running 6.2.0 or higher that are managed by a Control Center using firmware 6.0.X or 6.1.X must complete a dummy change in the security policy after enabling the URL Filter in the General Firewall settings.

Control Center

Add a Host Firewall rule to allow incoming connections on TCP/UDP port 888 to the Service IP. NextGen Secure Connectors will use this port to connect to the NextGen Control Center.

Step 3. Start the update

Now you can update the NextGen Firewall F-Series or Control Center.

For more information, see Updating F-Series Firewalls and Control Centers.