Threat Grid Appliance Offline Update Process

Created: 4/19/2018

Updated: 5/30/2018

Cisco Systems, Inc. www.cisco.com

Threat Grid Appliance Offline (Airgapped) Update Process

Most Threat Grid appliances are connected to the Internet and thus use the online update process. However, some of our customers maintain their Threat Grid appliances strictly within internal networks, that is, "airgapped". We do not recommend keeping appliances airgapped because doing so makes them less effective; however, this tradeoff may be necessary to support additional security or regulatory requirements.

For those users who run their Threat Grid appliances unconnected to the Internet, we provide the offline update process described in this document. Update media is provided by Threat Grid Support upon request, see below for details.

Overview

- **Media:** Airgap (offline) update media is provided by Threat Grid Support as an ISO, which can be copied to either a USB media, or (possibly) burned to read-only optical media should any of adequate size be available.
- **Size:** The size depends on which versions the update media supports, but it is certain to be several tens of gigabytes when new VMs are introduced between source and destination releases. For example, the media to upgrade from Threat Grid appliance version 2.2.3 to 2.4.1 is currently just under 70GB.
- **Upgrade Boot Cycle:** Each time the airgap update media is booted, it will determine the next release to upgrade to, and copy the content associated with that next release onto the appliance. A given release **may** also initiate a package installation, if that release does not have any prerequisite checks that must be run while the appliance is running. If the release includes such checks, or an override to portions of the update process that could add such checks, then the update will not actually apply until the user logs into OpAdmin and invokes the update with **OpAdmin > Operations > Update Appliance**.
- **Pre-Installation Hooks:** Depending on whether any pre-installation hooks are present for that specific upgrade, it will either run the upgrade immediately, or reboot the appliance back into its regular operating mode to allow the user to enter the usual administrative interface and start that upgrade by hand.
- **Repeat As Needed:** Each such media boot cycle will thus upgrade (or prepare to upgrade) only one step towards the eventual target release; the user must boot as many times as necessary to upgrade to the desired destination release.

Limitations

- CIMC vmedia is not supported for airgapped updates.
- Due to licensing constraints on 3rd-party components used, upgrade media for 1.x releases will no longer be available after UCS M3 hardware has hit EOL (end-of-life). It is thus critical that UCS M3 appliances either be replaced or upgraded prior to EOL.

Requirements

- **Migrations:** If the release notes for releases covered include scenarios where it is mandatory for a migration to take place before the next version is installed, the user must follow these steps before rebooting again to avoid putting their appliance in an unusable state.

  NOTE: The first 2.1.x release newer than 2.1.4 in particular will run several database migrations. It is *unsafe* to continue until these migrations are complete. For more information, see the *Threat Grid Appliance 2.1.5 Migration Note*.

- **Customer Info:** If starting from a release prior to 2.1.3, airgap upgrade media uses an encryption key derived from the customer’s individual license, and thus needs to be customized on a per-appliance basis. (The only user-visible effect is that with media built to support pre-2.1.3 origin versions, Threat Grid needs the licenses installed on those appliances beforehand, and the media won't work on any appliances not in the list for which it was built.)

  If starting with release 2.1.3 or after, the airgap media is generic and customer info is not needed.

Before You Begin

- **Backup.** You may want to consider backing up your appliance before you proceed with the update.
- Verify the current version of your appliance: **OpAdmin > Operations > Update Appliance**.
- Review the Threat Grid appliance version history in the Build Number/Version Lookup Table, which is available in all Threat Grid appliance documents: *Release Notes*, *Migration Notes, Setup and Configuration Guide*, and *Administrator's Guide*.
- Review the *Release Notes* and the *Migration Notes* in particular to anticipate any migration scenarios that may be included in the update.

To Update an Offline (Airgapped) Threat Grid Appliance

1. Contact Threat Grid Support: support@threatgrid.com, to request an offline update via support. This request should include the appliance serial number as well as the appliance build number.
2. Threat Grid will supply an updated ISO based on your installation.
3. Burn the ISO image to a bootable USB. Note that USB is the only supported device/method for offline updates.

   Linux:

   ```
   dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M
   ```

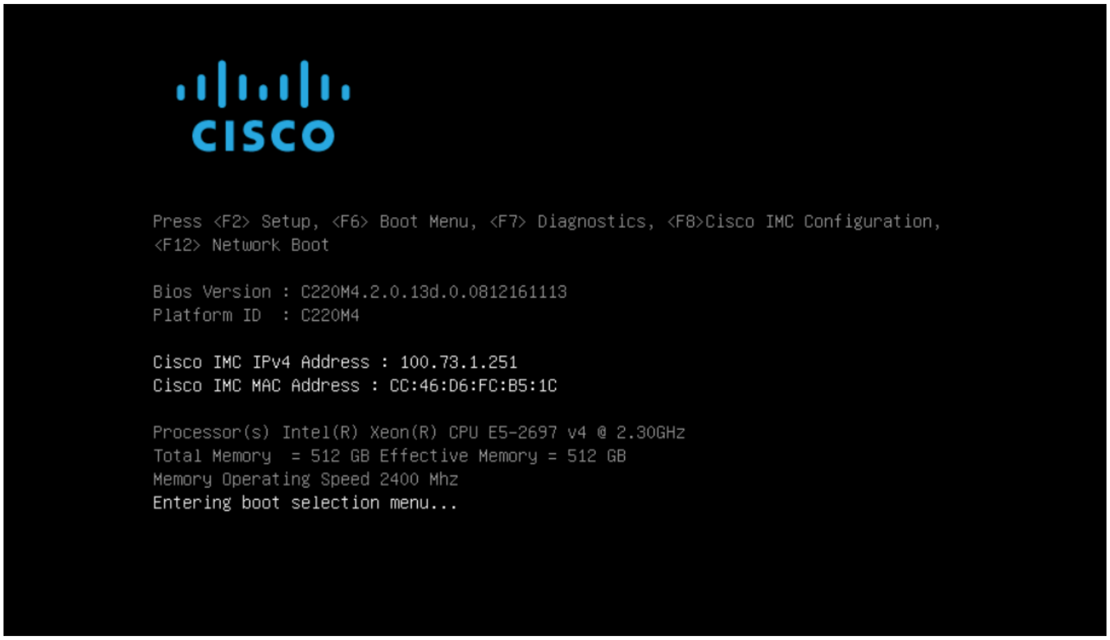
   Where <MY_USB> is the name of your USB key (leave off the angle brackets).

   Windows:

   Windows users please contact Threat Grid support for assistance with this task if necessary.
4. Insert the USB drive and turn on or reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu.

   You must be quick! You will only have a few seconds to make this selection. If you miss it, you will have to reboot and try again.

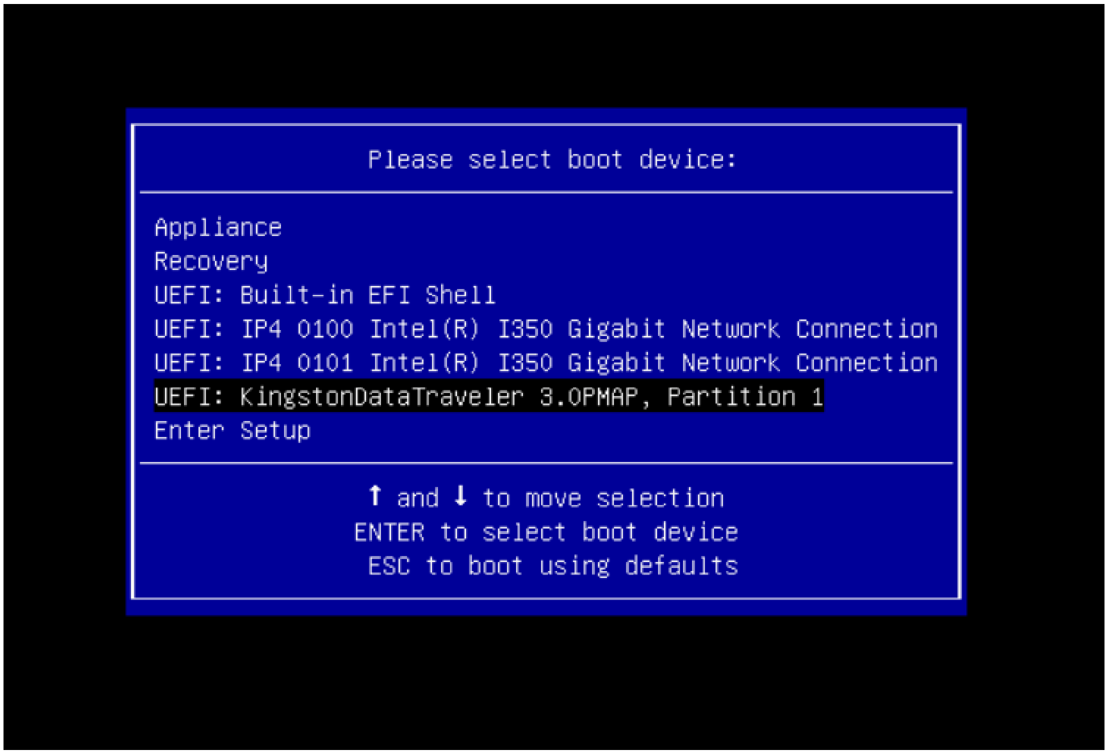
Figure 1 - Press F6 to Enter the Boot Menu



```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M4.2.0.13d.0.0812161113
Platform ID  : C220M4

Cisco IMC IPv4 Address : 100.73.1.251
Cisco IMC MAC Address : CC:46:D6:FC:B5:1C

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz
Total Memory  = 512 GB Effective Memory = 512 GB
Memory Operating Speed 2400 Mhz
Entering boot selection menu...
```

5. Navigate to the USB drive containing the update and press **Enter** to select:

Figure 2 - Select the Update USB



```
Please select boot device:

Appliance
Recovery
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection
UEFI: KingstonDataTraveler 3.0PMAP, Partition 1
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

The update media will determine the next release in the upgrade path, and will copy the content for that release onto the appliance. The appliance will either run the upgrade immediately, or reboot back into its regular operating mode to allow you to enter OpAdmin and start that upgrade manually.

6. Once the ISO boot process is completed, reboot the Threat Grid appliance back into operation mode.

7. Log into the portal UI and check for any warnings that speak to whether it's safe to upgrade, etc., before proceeding.

8. Go to the OpAdmin interface and apply the updates, *if they were not automatically applied during the reboot*:

   OpAdmin > Operations > Update Appliance

   NOTE: The update process will include additional reboots as a part of the update, which will not be made off of the USB media. For example, it's necessary to use the **Reboot** button on the installation page after updates are installed.

9. Repeat as needed for each version on the USB. See the following detailed example for more information.

An Example of the Offline Update Boot Sequence

If the appliance is currently at version 2.2.1, the update/reboot sequence to reach version 2.4.2 will look like this:

2.2.1 to 2.2.4

Minor releases will be included if the online update process includes them, otherwise they will be skipped.

Minor releases 2.2.2 and 2.2.3 are skipped.

- Ensure that the system has been in operation for at least 15 minutes since the last reboot to allow all self-tests to complete.
- Log into the Portal UI and check for any update-related warnings; resolve before continuing.
- Insert the bootable USB.
- Reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu, and select the USB media from the boot menu.
- Contents for 2.2.4 are copied from the USB onto the appliance. Reboot back into operation mode. Because 2.2.4 does not contain any update-process overrides, the packages will be installed at boot time, so no further steps are needed for this update.

2.2.4 to 2.3

- Ensure that the system has been in operation for at least 15 minutes since the last reboot to allow all self-tests to complete.
- Log into the Portal UI and check for any update-related warnings; resolve before continuing.
- Reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu, and select the USB media from the boot menu.
- Contents for 2.2.4 are copied from the USB onto the appliance. Reboot back into operation mode. Because 2.2.4 does not contain any update-process overrides, the packages will be installed at boot time, so no further steps are needed for this update.

2.3 to 2.3.3

- Ensure that the system has been in operation for at least 15 minutes since the last reboot to allow all self-tests to complete.
- Log into the Portal UI and check for any update-related warnings; resolve before continuing.
- Reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu, and select the USB media from the boot menu.
- Contents for 2.3.3 are copied from the USB onto the appliance. Reboot back into operation mode. Because 2.3.3 does not contain any update-process overrides, the packages will be installed at boot time, so no further steps are needed for this update.

2.3.3 to 2.4

- Ensure that the system has been in operation for at least 15 minutes since the last reboot to allow all self-tests to complete.
- Log into the Portal UI and check for any update-related warnings; resolve before continuing.
- Reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu, and select the USB media from the boot menu.
- Contents for 2.4 are copied from the USB onto the appliance. Reboot back into operation mode. Because 2.4 does not contain any update-process overrides, the packages will be installed at boot time, so no further steps are needed for this update.

2.4 to 2.4.2

Note that on customer request, update media may be built to stop at a different release (for example, 2.4.1). However, as of this writing, 2.4.2 is the latest release on the 2.4 line, and is the destination of an upgrade from any prior 2.4.x release on media not so customized.

- Ensure that the system has been in operation for at least 15 minutes since the last reboot to allow all self-tests to complete.
- Log into the Portal UI and check for any update-related warnings; resolve before continuing.
- Reboot the appliance. At the Cisco boot up screen, select "F6" to enter the Boot Menu, and select the USB media from the boot menu.
- Contents for 2.4.2 are copied from the USB onto the appliance. Reboot back into operation mode. Because 2.4.2 does not contain any update-process overrides, the packages will be installed at boot time, so no further steps are needed for this update; and because this is the last update included on the hypothetical media used for this example, no further actions are needed.

Support

If you have any questions about updating an offline appliance, please contact Threat Grid Support: support@threatgrid.com. Thank you!