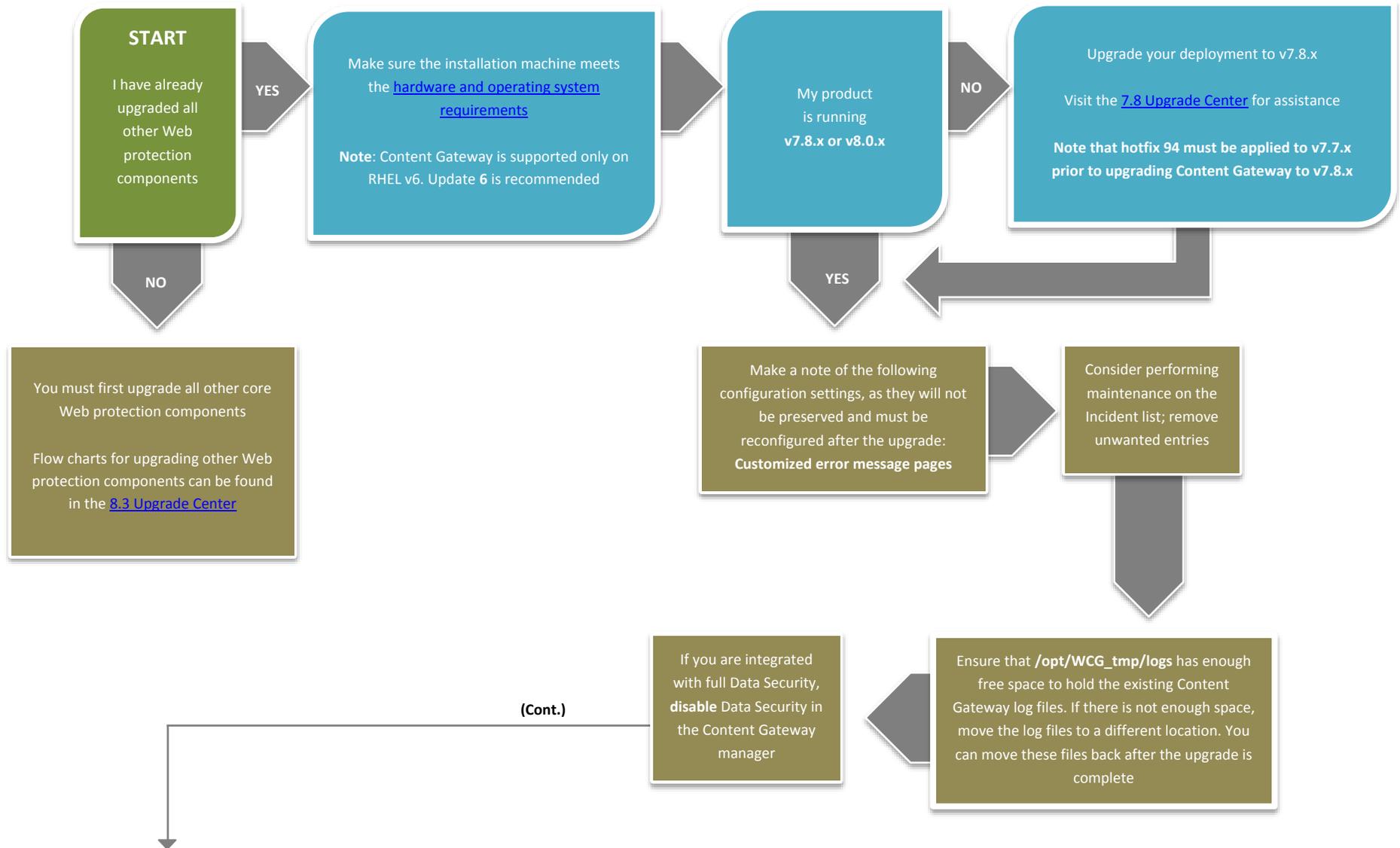


Upgrading Content Gateway from v7.8.4, v8.0.x, v8.1.x, or v8.2.x to v8.3.x

Review the v8.3x Release Notes prior to upgrade. For detailed upgrade instructions see the [Deployment and Installation Center](#)

BEFORE UPGRADE



Log on to the Content Gateway host and acquire root permissions with the command:
`su root`

Disable any currently running firewall on this machine

If SELinux is enabled, set it to permissive, or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled

Download the Content Gateway version 8.3.x installer from the My Account page at forcepoint.com and save it to a temporary directory

Unpack the Content Gateway installer tar archive. In the **same** directory, start the installation/upgrade script with the command:
`./wcg_install.sh`

Respond to the prompts. Up to the point that you are prompted to confirm your intent to upgrade, you can quit the installer by pressing CTRL+C. If you change your mind after you choose to continue, **do not** use CTRL+C to stop the process. Instead, allow the installation to complete and then uninstall

IMPORTANT:

During the upgrade, you are asked if you would like to use the previous installation selections. It is **highly** recommended you choose yes. When it asks if you would like to restore proxy settings after install, choose yes again. Selecting "no" at either of these points results in a fresh install

If at any point you receive errors, it may be because you need additional 64-bit libraries, which are included in the Content Gateway distribution. See the **upgrade guide** for further instructions, then return here

Re-enable the firewall on this machine. Be sure to open the ports used by Content Gateway
Refer [here](#) for assistance

If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to `/opt/WCG/logs` and delete the files in the temporary location

Register Content Gateway nodes in the Web Security manager on the **Settings > Content Gateway Access** page. Registered nodes add a link to the Content Gateway Manager logon portal and provide a visual system health indicator: a green check mark or a red X

If TRITON AP-WEB and TRITON AP-DATA are deployed together, after both have been upgraded to version 8.3.x, go to **Settings > Deployment > System Modules** on the Data tab of TRITON Manager, delete older instances of Content Gateway, and click **Deploy**

Read the Release Notes to learn about new features that can be configured post-upgrade

END

Reconfigure settings that were not able to be preserved over the upgrade process, and check other settings that may have changed. See the **upgrade guide** for more information

If you are integrated with full TRITON AP-DATA, re-register the appliance with the Data module in the Content Gateway manager