Release Notes

for Websense Web Filter, Web Security, and Web Security Gateway | v7.6.7

Topic 55350 / Updated: 31-August-2012

Applies To:	Web Filter 7.6.7 Web Security 7.6.7 Content Gateway 7.6.7 Web Security Gateway 7.6.7 Web Security Gateway Anywhere 7.6.7 V-Series Appliance 7.6.7

Version 7.6.7 is a stability patch for on-premises Websense Web security solutions. It rolls up many resolved customer issues for the v7.6.x series. This patch release is recommended for all sites.

Use these Release Notes to find information about what's changed and improved in version 7.6.7.

- *Installation and upgrade*
- *Content Gateway Operation tips*
- *Resolved and known issues*

Installation and upgrade

Topic 55351 / Updated: 31-August-2012

Applies To:	Web Filter 7.6.7 Web Security 7.6.7 Content Gateway 7.6.7 Web Security Gateway 7.6.7 Web Security Gateway Anywhere 7.6.7 V-Series Appliance 7.6.7

Always perform a full backup of all servers and save the backup files to a secure location, before upgrading to a newer version of Websense solutions.

All customers using Websense V-Series appliances (new sites as well as existing customers) need to apply the appliance patch. (Version 7.6.7 is not shipped from the factory with new appliances. You need to apply the patch.)

- Sites using Websense V-Series appliances should update all machines in the correct sequence, with the policy source (Policy Broker) first, and the TRITON management console last.
- The TRITON management console and Log Server are installed off the appliance, on Windows servers.

All server machines running Websense components in your network should be updated to 7.6.7. This includes all appliances, the TRITON management console machine, the Log Server machine, and all other servers running components. End-point machines (client machines) need not be updated.

Some older product versions require two or more steps for upgrade (see table below). In that case, download any transitional installers or patches that you need for the initial upgrade steps.

Please see the online Deployment and Installation Center for instructions on installing and deploying Websense Web security products at v7.6.7.

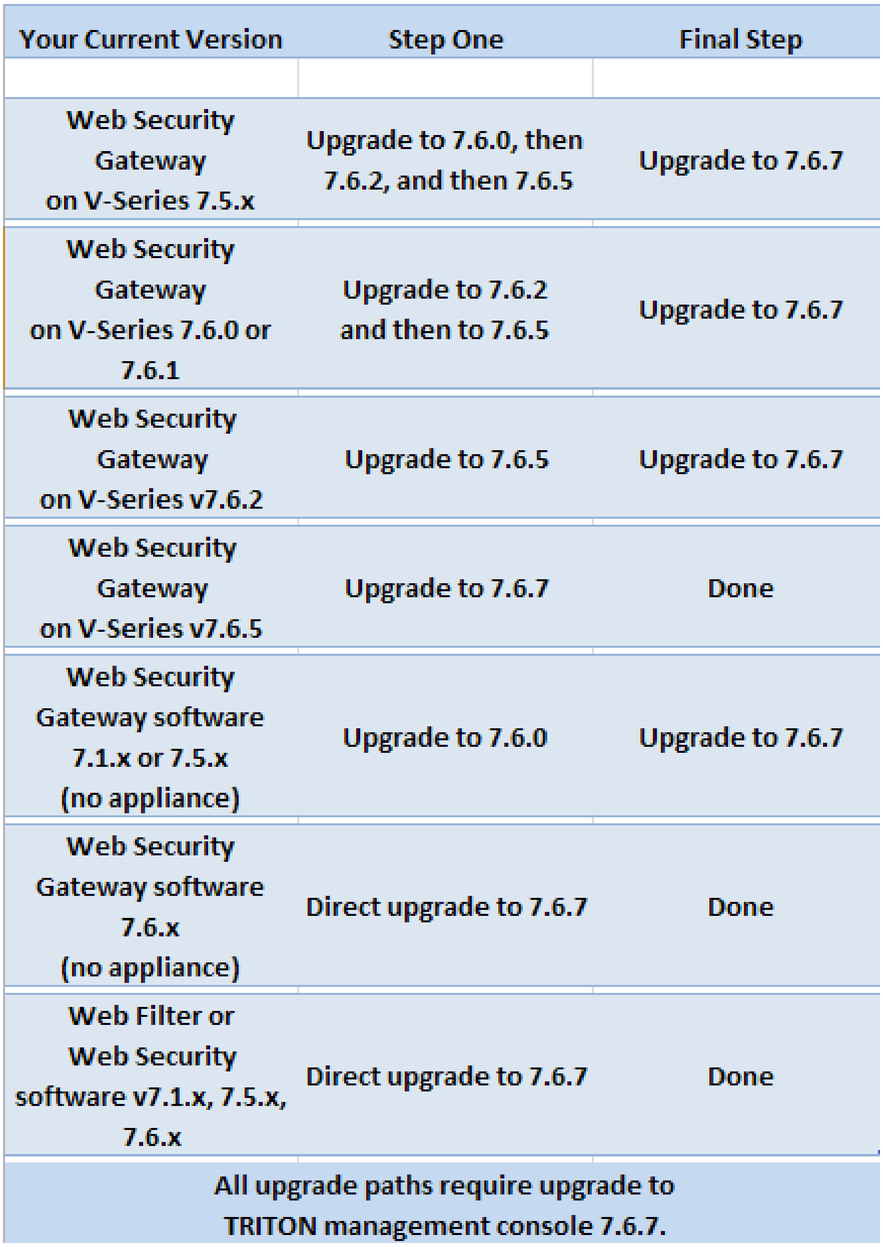
Refer to the Upgrade Center for instructions about upgrading to v7.6.7 from a previous version. The upgrade follows standard Websense upgrade processes.

To obtain the v7.6.7 patch for your Websense V5000 G2 or V10000 G2 appliance:

1. Launch the Logon Portal that offers access to Appliance Manager by pointing a supported browser to:

   http://<IP-address-of-appliance-interface-C>
2. Log on to **Appliance Manager**. The user name is **admin**.
3. Go to the **Administration > Patch Management** page to check for patches, download them, and install them.
4. Appliances automatically check for patches once a day.
5. Check for patches at any time with the **Check for Patches** button.
6. When a new patch is available, the patch version number, description, and status are displayed in the **Available patches** table.
7. After a patch is downloaded, it can be copied to another location on your network, where it can be easily and efficiently uploaded to one or more appliances.
8. The **Patch History** table shows patches already applied to the appliance.

Upgrade sequence



Your Current Version	Step One	Final Step
Web Security Gateway on V-Series 7.5.x	Upgrade to 7.6.0, then 7.6.2, and then 7.6.5	Upgrade to 7.6.7
Web Security Gateway on V-Series 7.6.0 or 7.6.1	Upgrade to 7.6.2 and then to 7.6.5	Upgrade to 7.6.7
Web Security Gateway on V-Series v7.6.2	Upgrade to 7.6.5	Upgrade to 7.6.7
Web Security Gateway on V-Series v7.6.5	Upgrade to 7.6.7	Done
Web Security Gateway software 7.1.x or 7.5.x (no appliance)	Upgrade to 7.6.0	Upgrade to 7.6.7
Web Security Gateway software 7.6.x (no appliance)	Direct upgrade to 7.6.7	Done
Web Filter or Web Security software v7.1.x, 7.5.x, 7.6.x	Direct upgrade to 7.6.7	Done
All upgrade paths require upgrade to TRITON management console 7.6.7.		

Content Gateway Operation tips

Topic 50359 / Updated: 31-August-2012

Applies To:	Websense® Content Gateway 7.6.7 Websense Web Security Gateway 7.6.7 Websense Web Security Gateway Anywhere 7.6.7

Installation file path and file ownership

Content Gateway is installed in /opt/WCG. The installation script does **not** prompt for an alternate location. If Content Gateway is being upgraded and the existing installation location is **not** /opt/WCG, the location is automatically moved to /opt/WCG by the upgrade program.

Content Gateway files are installed with root ownership. Content Gateway processes are run as root. The “Websense” user is no longer used.

With explicit proxy setup, send HTTPS traffic to port 8080

For Content Gateway sites with explicit proxy deployments, when SSL is enabled, browsers should be configured to send HTTPS traffic to the proxy on port 8080. The **ipnat.config** rule that was used to redirect traffic from 8070 to 8080 has been removed.

CR 35406 Fixed.

Client browser limitations

Not all Web browsers fully support transparent authentication (no-prompt).

Internet Explorer 7, 8, and 9

- Full support of transparent authentication

Mozilla Firefox 3 and 4

- Full support of transparent authentication

Google Chrome 6, 7, 8, 9, and 10

- Transparent authentication supported with IWA
- Not supported with Legacy NTLM; always challenges users for credentials

Opera 10

- Transparent authentication **not** supported; always challenges user for credentials
- HTTPS with IWA not supported.

Windows Safari 5 and Safari for iPad iOS 4

- Transparent authentication not supported; always challenges users for credentials
- When SSL Manager is enabled, HTTPS pages are only partially displayed

Software installation requires Internet connectivity

The Content Gateway host computer should have Internet connectivity before you start the software installation procedure. The software will install without Internet connectivity, but Websense license keys (and licensed features) cannot be validated until Internet connectivity is available.

Data Security integration

Websense Content Gateway v7.6.7 includes v7.6.3 of the Data Security policy engine. Customers must upgrade to Data Security v7.6.3 or a higher version of 7.6.x before upgrading to Content Gateway v7.6.7.

Websense Content Gateway v7.6.7 is not compatible with Data Security v7.7.

Cache size

Proxy cache size should be restricted to 147 GB. This size provides optimal resource utilization while also providing an excellent end-user experience. Because today's Internet sites are often composed of dynamic, uncacheable content, caching is a less significant factor in the end user's Web browsing experience.

Proxy ‘admin’ password restrictions

The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower-case letter, number, special character.

The password **cannot** contain the following special characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Port configuration

A full deployment of Content Gateway requires that several ports be open. See the Default Ports List for information about open ports and the reassignment of ports, if necessary.

Virtual IP address must not match any real IP address

For Content Gateway sites, when you are configuring the Virtual IP feature, make sure that the Virtual IP addresses do not conflict with any existing IP addresses assigned to the system.

Restart the proxy after protocol settings change

Any time you change your protocol settings in Content Gateway Manager (for example, with **Configure** > **SSL** > **Decryption/Encryption** > **Inbound** > **Protocol Settings**), you must restart the proxy for the new settings to take effect.

Reverse proxy

Content Gateway **does not** function as a reverse proxy.

Accessing Intranet sites in an explicit proxy deployment

For sites using Content Gateway, if your clients cannot access your Intranet sites, verify that your operating system has been correctly configured to resolve all internal and external hostnames. Use the **nslookup** command to verify that a domain is listed in your DNS server:

For internal-facing servers:

```
nslookup intranet.mycorp.com
```

For external Web sites:

```
nslookup www.websense.com
```

If your organization has multiple DNS domains, verify that a hostname in each domain resolves correctly. If you are unable to resolve hostnames, verify the contents of the **/etc/resolv.conf** file, which provides search rules for how domain names are resolved in DNS.

When Content Gateway is on a V-Series appliance, the domain of the hostname is automatically added to **/etc/resolv.conf**. For example, if the hostname of the appliance is vseries.example.com, then Content Gateway treats “intranet” requests as “intranet.example.com”.

Resolved and known issues

Topic 50352 / Updated: 31-August-2012

Applies To:	Web Filter 7.6.7 Web Security 7.6.7 Content Gateway 7.6.7 Web Security Gateway 7.6.7 Web Security Gateway Anywhere 7.6.7

A separate list of Resolved and Known issues for this release is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, each link below takes you to a login prompt. Log in to view the lists.

- Web Filter / Web Security
- Websense Content Gateway