Upgrading a V-Series Appliance to version 7.7

Websense Support Webinar October 2012
Title:
  – Support Specialist

Accomplishments:
  – 10 years supporting Websense products

Qualifications:
  – Technical Support Mentor
  – Product Trainer
Goals and Objectives

- V-Series appliance upgrade
  - Pre-upgrade activities
  - Post-upgrade activities
- Upgrading Websense off-appliance components
- Upgrade path
- Order for upgrading Websense components
- Backup
- Best practice check list
- Demonstration
Upgrading to v7.7

• Versions 7.6.0, 7.6.1, 7.6.2, 7.6.5 may upgrade
  – Email Security Gateway (Anywhere)
  – Data Security, v7.6.0, v7.6.2 and v7.6.3

• Non-appliance components
  – Version 7.5.x or v7.6.0-7.6.5 may directly upgrade

• Earlier versions must first upgrade to either v7.6.0, 7.6.1, 7.6.2, or 7.6.5
Patch, Upgrade, and Recovery Image

- **Patches** and **upgrades** preserve configuration settings
  - Typically does not require updating other components

- **Patch**
  - Typically does not require updating other components

- **Upgrade**
  - Includes enhancements and results in raising your product version level
  - All components must be same version level

- **Recovery Image**
  - Erases all software modules, all data, and all settings
  - Restores the appliance to factory settings
V7.7 System Requirements

- TRITON management server
  - On V-Series appliance (evaluations only)
  - Windows Server 2008 32-bit (Web Security only)
  - Windows Server 2008 R2 64-bit (best practice)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Security</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Email Security</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Hardware requirements increase when
  - Running SQL Server locally
  - Installing additional management modules
- Requirements range from 4-8 cores and 4-16 GB RAM
V7.7 System Requirements

- TRITON management console browser support

<table>
<thead>
<tr>
<th>Browser</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>8* and 9</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>4.x through 13.x</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>13 and later</td>
</tr>
</tbody>
</table>

* For Internet Explorer 8 only, do not use compatibility mode.

- Virtualization
  - All TRITON Unified Security Center components
    - Hyper-V over Windows Server 2008 R2
    - VMware over Windows Server 2008 R2
V7.7 System Requirements

• Reporting database
  – Microsoft SQL Server 2008 R2 Express
    • May reside locally on TRITON management server
    • Best for evaluations and small deployments
    • Install SQL Express only via the Websense installer
  – Microsoft SQL Server, Standard or Enterprise version
    • May NOT reside locally on TRITON management server

<table>
<thead>
<tr>
<th>Supported Database Engines</th>
<th>Data Security</th>
<th>Web Security</th>
<th>Email Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2005 SP4*</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SQL Server 2008**</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SQL Server 2008 R2 Express</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SQL Server 2008 R2***</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
V7.7 System Requirements

• Websense software components
  – Not supported on domain controllers
  – Most Web Security components are supported on
    • Windows Server 2008 (32-bit) and 2008 R2 (64-bit)
    • Red Hat Enterprise Linux 5 and 6

• Websense Content Gateway
  – Linux only
  – Red Hat Enterprise Linux 5 or 6

• For complete system requirements, see
  – Deployment and Installation Center v7.7
High Level Upgrade Scenario

• Upgrading TRITON Infrastructure, Web Security, Data Security, and Email Security
  – Policy Broker resides on V-Series appliance and additional Websense components are located off appliance
    • Obtain downloads
      – Appliance upgrade rpm
      – Websense TRITON Unified Installer
    • Collect backups
    • Perform pre-upgrade steps
    • Upgrade primary appliance
    • Upgrade secondary appliance(s)
    • Upgrade off-appliance Websense components
    • Perform post-upgrade steps
    • Verify upgrade was successful
1. **Email Log Server** (only if installed alone)
2. **Policy Broker**
3. **Policy Server(s)**
4. **Filtering Service** or **User Service**, and **Directory Agent**
5. **Email Security mode** only appliance
6. **Web Log Server**, **Sync Service**, and **Email Log Server** (when installed with other Websense components)
7. **TRITON management server** (TRITON Infrastructure)
   - **Web Security** module
   - **Email Security** module
   - **Data Security** module
8. Other Web Security components
   - **Network Agent, Content Gateway** (software-based proxy), Logon Agent, DC Agent, RADIUS Agent, eDirectory Agent, and Remote Filtering Server

9. Filtering **plug-ins**
   - Citrix XenApp or Microsoft Forefront TMG

10. Other Data Security components
    - **Supplemental servers, SMTP agents, ISA/TMG agents, printer agents, protectors, and mobile agents**

11. Client components (any order)
    - **Remote Filtering Client, Logon Application** (LogonApp.exe), **Web Endpoint**, and **Data Endpoint**
Pre-upgrade Check List

- Websense MUST be a functioning system
- Review product Release Notes
  - Websense Web Security, Content Gateway, TRITON Unified Security Center, V-Series Appliance, and Websense Data Security
- Machines must meet hardware and OS recommendations
- Ensure power to the V-Series appliance is not interrupted
- Confirm your third-party component works with v7.7
  - Microsoft ISA Server is not supported
  - Squid Web Proxy Cache is not supported
  - Supported Citrix versions have changed
  - Blue Coat Proxy no longer supports traditional (on-box or off-box) integrations
  - Check Point and Cisco integration version requirements have changed
Pre-upgrade Check List

- Data Security user name and password is limited to 19 characters
- Record your DLP quick policies regulatory and compliance attributes
- Back up the Websense reporting databases
- Stop Web and Email Security Log Server services
- Disable all Websense SQL Server Agent jobs
- Preserve Content Gateway logs (optional)
- Record Content Gateway IWA settings
- Disable Content Gateway cluster
- Disable Content Gateway Virtual IP failover
Pre-upgrade Check List

- Record Network Agent settings (situational)
- Websense network administrator accounts must have a designated email address
- Disable the on-appliance TRITON - Web Security
- Back up Websense systems
- Close Windows Event Viewer
- Close all open applications
- Disable firewalls (Windows and Linux)
- Stop antivirus software
- Set service recovery properties to “Take No Action”
- Restart Websense services before starting upgrade
After saving the Full Appliance backup off to another machine, clear disk space by deleting backups.
Pre-upgrade Check List

- Open new firewall ports
  - Data Security Management Server, open 17500-17515
  - Email Security Gateway, open 17700-17714
Upgrade Considerations

• Cannot change configuration settings during upgrade
• Internet access may be disrupted
• Filtering Service downloads a new Master Database
• Personal Email Manager is not available during upgrade
• Cannot upgrade individual Websense components
• All components on a machine are upgraded in the correct order
• Cannot roll back a successfully upgraded component
• If Websense Log Server uses a Windows trusted connection with SQL Server, perform the upgrade logged on using same network account
Collecting Backups

- Full appliance configuration backup
- TRITON management server
- Web Security components
- Websense Content Gateway
- Email Security
- Data Security
Collecting Backups

• Full appliance configuration backup
  – Appliance Manager > Administration > Backup Utility > Perform Backup > Full Appliance Configuration
  – Click Run Backup Now
  – Move the backup file off the appliance

• Demonstration
Collecting Backups

• TRITON management server
  – On the TRITON management server machine
    • Start > All Programs > Administrative Tools > Task Scheduler > Task Scheduler Library
    • Ensure the TRITON Backup task is enabled
    • Right-click the TRITON Backup task and select Run
    • The C:\EIPBackup folder contains the backup data
  – Move the backup folder off the server
• Demonstration
Collecting Backups

- **Web Security components**
  - Do one of the following
    - **Windows**
      - Navigate to “\Websense\Web Security\bin” and run
        » wsbackup -b -d <directory>
    - **Linux**
      - Navigate to “/opt/Websense/bin” directory and run
        » export LD_LIBRARY_PATH=.
        » ./wsbackup -b -d <directory>
  - The destination folder must already exist
    - Move the backup files off the server
    - Repeat on all machines with Websense Web Security components
- **Demonstration**
Collecting Backups

• Websense Content Gateway
  – The Full Appliance Configuration backup includes Content Gateway module settings
    • When performing a Full Appliance Backup for recovery, it is not necessary to also generate a Content Gateway snapshot
  – Content Gateway Manager allows saving a snapshot
    • A snapshot saves the current running state of the Content Gateway module
    • Typically, you would use the Content Gateway Manager > Configure > My Proxy > Snapshots > File System option before making proxy setting changes
    • Restoring a snapshot allows for quickly recovering prior Content Gateway settings

• Demonstration - same as Full Appliance Backup
Collecting Backups

• Email Security
  1. TRITON - Email Security management server
     o **Settings > General > Backup/Restore > select Backup**
     o The C:\ESGBackup folder contains the backup data
  2. Appliance Manager console
     o **Administration > Backup Utility > Email Security Configuration**
     o Full Appliance Backup includes Email Security module
  3. TRITON - Data Security management server
     o **Task Scheduler**
  4. Microsoft SQL Server
     o Databases: esglogdb76, esglogdb76_n
     o SQL Agent Job: **Websense_ETL_Job__esglogdb76**
     o SQL Agent Job: **Websense_Maintenance_Job__esglogdb76**

• Demonstration
Collecting Backups

• Data Security
  – Configure backup settings in TRITON - Data Security
    • Settings > General > System > Backup
    • For Path and Credentials data, and including Forensics
  – TRITON - Data Security management server machine
    • Start > Administrative Tools > Task Scheduler > Task Scheduler Library > DSS Backup > Enable
    • Right-click DSS Backup and select Run
    • Confirm the backup completed successfully
      – Within the backup folder, C:\DSSBackup (default), confirm the DataBackup.log does not include the words ‘fail’ or ‘error’

• Demonstration
Collecting Backups

• Ensure all backup files are saved to a safe network location not located on any Websense system
Collecting Backups

- **Microsoft SQL Server**
  - **Email Security**
    - Databases: `esglogdb76, esglogdb76_n`
    - SQL Agent Job: `Websense_ETL_Job__esglogdb76`
    - SQL Agent Job: `Websense_Maintenance_Job__esglogdb76`
  - **Web Security**
    - Databases: `wslogdb70, wslogdb70_n`
    - SQL Agent Job: `Websense_ETL_Job__wslogdb70`
    - SQL Agent Job: `Websense_IBT_DRIVER_wslogdb70`
    - SQL Agent Job: `Websense_Maintenance_Job__wslogdb70`
  - **Data Security**
    - Database: `wbsn-data-security`
    - Database: `wbsn-data-security-temp-archive`
1. Ensure no administrator is logged into TRITON - Web Security management console

2. Restart the appliance

3. Download the upgrade patch

4. Click Install

5. When patch installation completes, restart the appliance

6. Verify V-Series version is v7.7
   - Appliance Manager > Configuration > General

7. Check time zone settings
   - Appliance Manager > Select System > Configuration

8. Upgrade remaining appliances

9. Upgrade off-appliance components
• Demonstration
• When upgrade completes, restart the appliance
  – When prompted, click Restart Now
  – Do not cycle the power
V-Series Appliance Upgrade

- During patch installation, a progress window displays the percentage of completion

  ![Progress Window](image)

  **Patch Installation - 7.7.0**

  Patch installation takes **approximately 5-10 minutes**. The appliance restarts automatically when installation is complete.

- Actual upgrade times are approximately
  - 20-30 minutes for Filtering only mode
  - 40-50 minutes for Web Security Gateway mode
  - 80-90 minutes for Web Filtering Gateway and Email mode
• If your network contains an Email only appliance
  – Upgrade all non-email appliances first
  – Upgrade the Email appliance before upgrading any off-appliance Websense components
  • Exception
    – When Email Log Server is the only Websense component installed on a server
Upgrading Multiple Appliances

- **Full policy source** resides on either a ‘Web’ mode or a combination ‘Web and Email’ V-Series appliance
  
  1. Upgrade the **Full policy source** V-Series appliance, and immediately restart
  
  2. Upgrade all **User directory and filtering appliances**, and immediately restart
  
  3. Upgrade all **Filtering only** appliances, and immediately restart
  
  4. After upgrading all appliances, upgrade off-box components

© 2012 Websense, Inc.
Upgrading Multiple Appliances

• **Full policy source** is NOT on a V-Series appliance

  1. Upgrade the Policy Broker system
  2. Upgrade all *User directory and filtering* appliances, and immediately restart
  3. Upgrade all *Filtering only* appliances, and immediately restart
  4. Upgrade off-appliance components
If the **Full policy source** appliance is unavailable

- Set the *User directory and filtering* or *Filtering only* appliance to temporarily be a **Full policy source**

- **Appliance Manager > Configuration > Web Security Components > Policy Source > Full policy source > Save**
Upgrading Multiple Appliances

- Upgrade to v7.7 and immediately restart
- When the original *Full policy source* appliance becomes available again and is running v7.7
  - Change the upgraded temporary *Full policy source* machine, pointing it back to the original *Full policy source* appliance
    - Appliance Manager > Configuration > Web Security Components > Policy Source > User directory and filtering (Filtering only) > enter primary appliance’s IP address > Save
- Upgrade remaining off-appliance components
Post Upgrade Check List

- Machines must be rebooted to complete upgrade
- All components must be the same version
- Exclude Websense folders from antivirus scans
- Restart antivirus, firewall, etc.
- Enable the SQL Server Agent jobs
- Integrations may require additional upgrade steps
  - Integrating Web Security with Check Point, page 445
  - Integrating Web Security with Cisco, page 481
  - Integrating Web Security with Citrix, page 513
  - Integrating Web Security with Microsoft Products, page 535
  - Installing Web Security for Universal Integrations, page 563

  • NOTE: Overtime, the page numbers above will change somewhat as the referenced document is updated
Post Upgrade Check List

- Repair Email Security Gateway (Anywhere) registration with Data Security

1. **TRITON - Email Security** > Settings > General > Data Security, click Unregister

2. **TRITON - Data Security** > Settings > Deployment > System Modules > Email Security Gateway registration > Delete the older instance > click Deploy

3. **TRITON - Email Security** > Settings > General > Data Security
   - Register the Email Security appliance with Data Security

4. **TRITON - Data Security** > click Deploy

5. Verify
   - Redirect email traffic through V-Series appliance
Post Upgrade Check List

- Register appliance with Web Security Policy Server
  - TRITON - Web Security > Settings > Policy Servers > add the appliance
  - TRITON console > Appliances tab > register the appliance

- Register Content Gateway nodes
  - TRITON - Web Security > Settings > Content Gateway Access page

- Configure Content Gateway system alerts
  - TRITON - Web Security > Settings > Alerts > System page

- Clear browser cache for new management console
Post Upgrade Check List

- TRITON Unified Security Center management console requires importing new security certificate
- Restore Network Agent settings
- Restore IWA settings
- Enable proxy cluster
- Enable Virtual IP failover
- Clients may need to re-import Root CA
  - In v7.7, the default Root CA presented to clients is SHA-1
  - Prior to v7.7, the Root CA was signed with a MD5 hash
• Before upgrading Web, Email, and Data Security
• Upgrading V-Series Appliances to v7.7
• Upgrading solutions that include Web, Email, and Data Security
• Backing up and restoring your Websense data
• Backup and Restore FAQ
• Deployment and Installation Center
• Release Notes
  – Websense Web Security
  – Websense Content Gateway
  – TRITON Unified Security Center
  – V-Series Appliance
  – Websense Data Security
  – Email Security Gateway
Upcoming Webinar

Title:
Quick Start 1: Web Security Configuration and Setup

Date:
November 14th, 2012

Time:
8:30 A.M. PDT (GMT -8)

How to register:
http://www.websense.com/content/SupportWebinars.aspx
Training

• To find Websense classes offered by Authorized Training Partners in your area, visit:
   http://www.websense.com/findaclass

• Websense Training Partners offer classes online and onsite at your location.

• For more information, please send email to:
   readiness@websense.com