v8.1 Release Notes for Websense Web Protection Solutions

Topic 51340 | Release Notes | TRITON AP-WEB and Web Filter & Security | 12-Oct-2015

Use the Release Notes to find information about what's new and improved for Websense® TRITON® AP-WEB and Web Filter & Security in version 8.1.

For information about Websense endpoint client software, please refer to the Release Notes for TRITON AP-ENDPOINT.

> **Note**
> The Websense Content Gateway component is not included in Web Filter & Security deployments. Content Gateway information applies only to TRITON AP-WEB.

Refer to the following when installing or upgrading to v8.1.

- Installing TRITON AP-WEB
- Installing Web Filter & Security
- When upgrading Websense TRITON Web Security Gateway/Anywhere or v8.0.x TRITON AP-WEB see TRITON AP-WEB
- Upgrade Web Filter *or* Web Security or v8.0.x Web Filter & Security see Web Filter & Security
- Deployment and Installation Center

> **Important**
> **V-Series appliance users:**
>
> Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher.
>
> See V-Series appliances supported with version 8.0

New in Websense Web Protection Solutions

Topic 51341 | Release Notes | TRITON AP-WEB and Web Filter & Security | 12-Oct-2015

The TRITON Settings Help, TRITON AP-WEB Administrator Help, and Content Gateway Help are available in Japanese as well as English for 8.0.x. The language selection for Help for modules of TRITON Manager (including TRITON AP-WEB) can be changed on the **TRITON Settings > My Account** page. The language selection for Content Gateway Help can be changed on the **Configure > My Proxy > UI Setup > General** page in the Content Gateway manager.

TRITON APX

Version 8.0 was the first product release that used a new, simplified product naming and grouping of the familiar Websense TRITON product line.

Original Name	New Name
Websense Web Filter	Websense Web Filter & Security
Websense Web Security	Websense Web Filter & Security
Websense TRITON Web Security Gateway	Websense TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	Websense TRITON AP-WEB with: • Web Hybrid Module • Web DLP Module • Web Sandbox Module

Previous product functionality remains intact. The user interface has the same familiar look and feel and the core product continues to provide the strong protections you've come to rely on.

In addition to new names introduced with v8.0, our web protection solutions offer new features and includes product corrections. Refer to the information provided in these Release Notes for additional product information.

File Sandboxing control

Additional File Sandboxing options have been added to the Web module of the TRITON Manager.

File Sandboxing control options

The **Web** > **Settings** > **Scanning** > **Scanning Options** page of the Triton manager includes new options for File Sandboxing. Now, when you enable File Sandboxing, you can specify file types that should not be submitted.

- Check the box next to the general file types listed to keep those file types from being sent to the file sandbox. By default, none of the boxes are checked; all suspicious files are sent.

  Note that analysis is performed to determine a file's true type.

  When a file type is selected for "Do not submit", both the true file type and the file extension are used to determine that the file will not be sent to the file sandbox.

  Caution: Electing not to send file types to the sandbox may expose the network to unknown risk. Select the file types based on proper risk assessment. Balance the privacy risks involved in sending files to the sandbox against the security risks involved in not sending them.
- To not send files having a specific extension, check **Files with the following extensions** and enter file extensions in the input box provided. Multiple file extensions can be added in a comma separated list. Click **Add** to populate the list below the entry field.

  Highlight a file extension and click **Delete** to remove the entry from the list.

Text has also been added to the **Scanning Options** page to better explain which features impact File Sandboxing. At least one of the following options must be enabled for files to be sent to the sandbox:

- Content Categorization
- Security Threats: Content Security
- Advanced Detection
- Antivirus Scanning

Endpoint and Hybrid configuration options available in TRITON Manager

Certain options and features that were previously only available to Cloud Web Security customers have been added to the Web module of the TRITON Manager for use with the Web Hybrid module.

Endpoint options

After you **Enable TRITON AP-ENDPOINT Web installation and update on client machines** on the **Settings > Hybrid Configuration > Hybrid User Identification** page, you can now configure:

- Version updates by operating system.

  In previous versions of TRITON AP-WEB, version updates were configurable, but would be done on all client machines. With this version, you can ensure that endpoints on your Windows or Mac client machines always have the latest version of the endpoint client software when it is available.

  1. Under **Version Update**, check the box next to the operating system that you want to be automatically updated.
  2. Click **OK**, then **Save and Deploy** to save your changes.

  If you later remove the check from one or both boxes, endpoint updates will no longer be applied to client machines using that operating system. Existing endpoint installations will, however, continue to work.

- A list of applications that should bypass endpoint policy enforcement.

  Some applications do not work properly with endpoint enforcement. The Application Bypass option allows you to add a list of applications that may be causing problems.

  Note that this feature does not work for applications that use system browser settings to determine a proxy. Also, you may need to update your endpoint deployments. End users must have at least endpoint build 1138 (Windows) or 1566 (Mac) to use application bypass.

  1. Click **Add** under Application Bypass to open the **Add Applications** window.
  2. Specify the operating system for the Application(s) you wish to add.
  3. Enter the Application(s) in the field provided.
     - Enter a single application or a comma-separated list of applications.
     - Include the file extension for each application. If no extension is entered, the application name is treated like a regular expression.
     - An asterisk (*) wildcard can be used in application names. For example, appl.*.
  4. Click **Add** to return to the **Hybrid User Identification** page and add your entry to the list.

     If there are any errors found in your entry, correct them and click **Add** again.
  5. Click **OK**, then **Save and Deploy** to save your changes.

  The Application Bypass list includes all of the applications you have added. Check the box next to an Application name and click **Delete** to remove it from the list.

Note also that the **Hybrid User Identification** page has been reorganized to group related items and clarify the relationship between them.

User Access options

New options are available when configuring hybrid user access on the **Settings > Hybrid Configuration > User Access** page.

- **Web Browsing Optimization**

  By default, end user web traffic is routed to the nearest cloud data center based on the egress IP address of your Domain Name Server (DNS). This may mean that traffic for users in a geographic location different from the DNS is not optimally routed, causing some latency issues.

  1. Select **Route traffic based on end users' egress IP** to re-route your web traffic to data centers based on the location of the end user, rather than your DNS.
  2. Click **OK**, then **Save and Deploy** to save your changes.

  I**MPORTANT NOTE:** If you are upgrading to v8.1 and Technical Support had enabled this feature for you in your previous version, please contact Technical Support before enabling this feature on the v8.1 **User Access** page.

- **Certificate Verification Bypass for HTTPS sites**

  The hybrid service verifies certificates for HTTPS sites that it has decrypted and analyzed. Certificate verification checks apply to all certificates in the trust chain. Use of certificate verification is recommended in order to avoid security risks from malicious sites with certificates that misrepresent their identity.

  If certificate verification fails, a notification page displays indicating that a certificate error has been detected. End users can be given the option to bypass certificate errors for specified sites. They can proceed to the site or go back.

  You can also create a list of sites that do not return a notification page for certificate errors. Instead the user is given access to the site. This option is useful, for example, for sites that you trust even if the certificate is expired, is not yet valid, or is self-signed.

  1. Click **On** under **Perform certificate verification** to enable the feature. Click **Off** to disable it.
  2. Select **Provide end users an option to bypass all certificate errors** to provide all users with the notification page that includes an option to bypass a certificate error and proceed to the site.
  3. If you have selected **Perform certificate verification**, you can maintain a list of domains or IP addresses for which certificate verification errors are automatically bypassed. The end user receives no notification page and is given access to the site.

     Enter the domains and IP addresses in the entry field provided.

     A comma-separated list can be used, but IP address ranges are not supported.

     Click **Add** to populate the list.

     Select an item on the list and click **Delete** to remove it.
  4. Click **OK**, then **Save and Deploy** to save your changes.

Improvements to Incremental Upgrade

The management console will now connect to a Policy Server whose version does not match the management console version. The Policy Server version must be one of these supported versions:

- v7.8.4
- v8.0
- v8.0.1
- v8.1

Policy Servers with one of these supported versions can also be used in the **Add Policy Server** and **Edit Policy Server** pages. Once a supported Policy Server has been added, the Policy Server **Switch** button can be used to connect to it.

The **Policy Server Map**, available in multiple Policy Server deployments, now includes the version of each Policy Server included in the map. This allows you to easily determine the version of each of your Policy Servers as you progress with the incremental upgrade.

There are new limitations with this new feature:

- When logged on to the Web module of the TRITON manager,
  - Help, Find Answers information, field labels, and error messages are based on the version of the management console, even when the connection is to a Policy Server with a different version.
  - Show Me How tutorials may not work correctly unless the Policy Server and management console versions match.
  - Some of the pages of the TRITON Manager may not be accessible if the Policy Server and management console versions do not match.
- When using the **Settings > Policy Server** page to add or edit a secondary policy server, Directory Services settings cannot be inherited from a primary Policy Server unless the Policy Server versions match.

  If the versions don't match, but the **Inherit from the primary Policy Server** option has been checked, the Directory Services settings for the secondary Policy Server are left available for entry. When it can be determined that the Policy Server versions match, the Directory settings are copied from the primary Policy Server to the secondary, and the settings for the secondary Policy Server are disabled.

  View the **Policy Server Map** to check the version of the primary and each secondary Policy Server.

For a complete list of "Limitations & restrictions" for incremental upgrades, see the Incremental Upgrade document.

Installation and Upgrade improvements

The installation and upgrade processes has been enhanced to do more pre-checking, remove some dependencies that are no longer needed, and lengthen the time allowed for existing services to stop before producing an error. These enhancements make the installation and upgrade processes smoother and more likely to be successful.

Pre-checking is done for:

- The operating system. An error message displays if the operating system is not support. The installation or upgrade will not continue.

Pre-checks that are specific to the upgrade process are:

- Determine if the Log Database jobs have been stopped. A message displays and the upgrade process will attempt to stop them if they were not manually stopped prior to the upgrade. If the upgrade process is not able to stop them, a second message displays and you will need to manually stop them. You do not need to exit the installer but can return and continue once the jobs are stopped.
- When Log Server is upgraded, check the version of the Log Database. If the Log Database has already been upgraded by a previous Log Server upgrade, the database jobs are not stopped and the process of upgrading the database is skipped.

Other enhancements include:

- Reduced memory usage when a Log Database is created or upgraded.
- Improvements to the process of stopping Websense services during upgrades.
- Improvements to the replica Policy Broker upgrade process.
- A re-design of the upgrade process for many of the back-end components to remove the dependency between all components and Policy Server. This added stability to the upgrade process.
- The restart of Log Database jobs at the end of the upgrade process. Improvements to the upgrade process on an appliance which will both speed up the process and increase the probability of success.

Logon application support

Logon Agent communicates with the logon application (LogonApp) on client machines to identify users as they log onto or off of Windows domains.

The logon application now supports the following operating systems:

- Mac OS X 10.10 (64-bit)
- Microsoft Windows 8.1 Update 1 (32-bit and 64-bit; Windows 8.1 RT is not supported)

For more information about Logon Agent and the logon application, see the Using Logon Agent for Transparent User Identification white paper.

Third-party platform and product support

All components

This version adds support for:

- Mozilla Firefox 40
- Google Chrome 44
- Microsoft SQL Server 2012 SP2 and 2014
- Active Directory in Windows Server 2012 R2

Note that installing web protection components on Windows Server 2012 or 2012 R2 requires Microsoft .NET Framework v3.5. Install .NET Framework v3.5 before running the TRITON Unified Installer.

Content Gateway

This version adds support for:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.6: 2.6.32-504
- the corresponding CentOS version

In addition, Content Gateway is certified on the following 64-bit platforms:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.5: 2.6.32-431

    Note

    Websense testing encountered a kernel bug in version 2.6.32-431 that can impact performance. However, Content Gateway features were tested on this version of the OS and passed the certification tests.

  - Kernel version for 6.4: 2.6.32-358
- V-Series appliances

Content Gateway is also supported on the corresponding CentOS versions, including update 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Support for the following version has been dropped with this release:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.3: 2.6.32-279

> **Important**
> Customers currently using Red Hat Enterprise Linux 6.3 will need to upgrade their operating system prior to upgrading the product.

Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

Only kernels listed above are certified or supported.

Websense, Inc. provides “best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

Websense recommends that Red Hat Enterprise Linux systems that host Content Gateway be registered with Red Hat Network and kept up-to-date with the latest security patches.

> **Important**
> You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel ABI.

> **Important**
> Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

For a complete platform requirements information, see System requirements for this version in the Deployment and Installation Center.

Resolved and known issues

Topic 51344 | Release Notes | TRITON AP-WEB and Web Filter & Security | 12-Oct-2015

A list of resolved and known issues in this release is available to TRITON AP-WEB and Web Filter & Security customers.

If you are not currently logged in to MyWebsense, clicking the link brings up a login prompt. Log in to view the list.