v8.0.0 Release Notes for Websense Web Protection Solutions

Topic 51120 | Release Notes | TRITON AP-WEB | 02-Feb-2015

Use the Release Notes to find information about what's new and improved for Websense® TRITON® AP-WEB in version 8.0.0.

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

Refer to the following when installing or upgrading to v8.0.

- Installing TRITON AP-WEB
- Upgrading Websense TRITON Web Security Gateway/Anywhere to TRITON AP-WEB

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 51121 | Release Notes | TRITON AP-WEB | 02-Feb-2015

Both the Administrator Help and Content Gateway Manager Help are available in both English and Japanese.

- For the Administrator Help in the TRITON Manager, select a language on the **TRITON Settings > My Account** page.
- For the Content Gateway Manager Help, specify the language on the **Configure > My Proxy > UI Setup > General** page.

TRITON APX

To address the wide-scale adoption of cloud and mobile technologies, along with a rapid growth in distributed workforces, Websense, Inc., is excited to launch a new, industry-leading security suite — Websense® TRITON® APX 8.0. This new modular platform provides advanced threat and data theft protection for organizations that wish to embrace new technologies and working practices. TRITON® APX provides protection across the entire kill-chain, reveals actionable intelligence, and enables real-time feedback to educate and motivate end users to avoid risky behavior. This product release is the culmination of eighteen months of business transformation and innovation. As a result, Websense customers are now able to maximize the unparalleled protection and ROI of Websense TRITON APX solutions well into the future.

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

Original Name	New Name
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, our web protection solutions offer new features and includes product corrections. Refer to the information provided in these Release Notes for additional product information.

Investigative Reports: Improved support for scheduling and exporting large reports

In prior versions, the amount of time to generate a PDF or Excel document in investigative reports could be excessive if:

- A scheduled report job produced a large report.
- A large report was exported.

Changes have been made to reduce the amount of time it now takes for these processes to complete.

There is also a change to the way some of the variables defined in the wse.ini file (found in C:/Program Files (x86)/Websense/Web Security/webroot/Explorer, by default) are used by scheduled report jobs.

- **sendMulti**, used to divide large, scheduled detail reports into multiple files, now uses the value defined in **reportBatchCount** to determine how many records to include in each file. Set the **sendMulti** value to 1 to enable the feature
- **reportBatchCount**, used to determine the number of records included in a scheduled report, can no longer be set to a value greater than 500,000.
  - The default value is 10,000.
  - This setting is used when **sendMulti** is enabled (1).
  - Any value over 500,000 is ignored and 500,000 is used.
- If **sendMulti** is disabled (0), each scheduled detail report is divided into files containing up to 500,000 records.
- Only detail reports use these wse.ini files settings.

To better accommodate emailing the scheduled reports, all reports are sent as a zip file, even when the report is a single file.

For the best performance, a minimum of 4G of RAM is recommended. Companies with large amounts of data should consider increasing to 8G or more.

Mobile Integration

TRITON AP-WEB customers with the Web Hybrid module now have the option to include Websense TRITON AP-MOBILE integrated with AirWatch® Mobile Device Management (MDM).

> **Important**
> If you purchase a subscription to TRITON AP MOBILE, at this time you may use TRITON AP MOBILE integrated with AirWatch Mobile Device Management (MDM), which is available on an Early Access as is basis, or TRITON Mobile Security. At the time of purchase, you'll need to indicate which product you wish to use, so that the TRITON Manager (cloud or hybrid) can be set up for that product.

TRITON AP-MOBILE protects your end users' devices from potential data loss and the possible theft of intellectual property, plus from mobile malware, web threats, phishing attacks, spoofing, and more—all of which helps them safely access corporate resources.

When integrated with AirWatch MDM, you can provision iOS and Android mobile devices to send traffic to the Websense cloud service for analysis and policy enforcement. You can also configure and update device settings over the air, create different policies for corporate versus personal devices, and secure mobile devices through actions such as locking and wiping them.

To set up your account, in the Web module of the TRITON Manager, go to the **Settings** > **Hybrid Configuration > Mobile Integration > Mobile Device Management Account Setup** page.

1. Select the checkbox **Integrate with MDM provider**.

   Note that unchecking this box and clicking Save Now disables integration between the Websense solution and AirWatch MDM.
2. Enter the API URL and API key. You need to obtain these from the AirWatch Console. See Step 4, Log on to the AirWatch Console in the Getting Started Guide.

   For the API URL, remove the "/API" from the end of the URL, so for example, change https://orgname.airwlab.com/API to https://orgname.airwlab.com.
3. Enter the user name and password that you use to log on to your AirWatch administrator account.
4. Click **Save Now**.
5. After you click Save Now, and the settings are confirmed and saved successfully, this page then displays a user name and password that have been automatically generated for your hybrid account, along with a connection URL.

Copy and paste these three items into the VPN connection information section of the AirWatch Console.

For an overview of the mobile integration process, see the Getting Started Guide.

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 includes support for:

- Internet Explorer 10, standards mode
- Internet Explorer 11, standards mode
- Mozilla Firefox 32
- Google Chrome 38

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

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:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.3: 2.6.32-279
- The corresponding CentOS versions, including updates 3 and 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

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 the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 8.0 Content Gateway installer.

Websense also 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 description of platform requirements, see *Requirements overview*.

Installing a Web Protection Solution

Topic 51122 | Release Notes | TRITON AP-WEB | 02-Feb-2015

Requirements overview

Except for the components listed immediately below, all web protection components can run on the following operating systems:

- Microsoft Windows Server 2008 R2, 2008 R2 SP1, 2012, or 2012 R2

> **Important**
> Before installing any components, make sure that .NET Framework 3.5 is installed on the machine.

- Red Hat Enterprise Linux 6.x(64-bit)

The following components run on Windows platforms only:

- TRITON Manager
- Linking Service
- Log Server
- DC Agent
- Real-Time Monitor

The following component runs on Linux 6.x platforms or Websense appliances only:

- Content Gateway

In appliance-based deployments, in addition to the Windows-only components, the following components, when used, must be installed off-appliance:

- Sync Service
- Transparent identification agents (eDirectory Agent, Logon Agent, RADIUS Agent)

To enable web reporting tools, use one of the following certified database engines:

- Microsoft SQL Server 2012 SP2 (or the latest service pack from Microsoft) Standard, Business Intelligence, or Enterprise

  Important

  SQL Server 2012 uses a different security model than previous versions. To successfully create the Log Database in SQL Server 2012, you must either:

  - Install the database in the default SQL Server folder.
  - Grant the database engine full control over the folder that will host the database before you install Log Server.

- Microsoft SQL Server 2008 SP3 (or the latest service pack from Microsoft) Standard or Enterprise
- Microsoft SQL Server 2008 R2 SP2 (or the latest service pack from Microsoft) Standard or Enterprise
- For very small networks and evaluation environments, SQL Server 2008 R2 Express SP 2 (packaged in the TRITON Unified Installer).

See System requirements for this version in the Deployment and Installation Center for detailed hardware and software requirements.

Installation overview

The number of steps required to install your software depends on the hardware platforms used in your environment, the size of your network, and how widely you plan to deploy components.

The Websense Deployment and Installation Center is the complete resource for deployment, installation, and upgrade information for version 8.0 TRITON Enterprise solutions.

As a best practice, for software component installation, log in as a domain and local administrator to run the installer.

See *Downloading the installer* for information on where to get the installation package you need.

TRITON AP-WEB

For a typical TRITON AP-WEB software deployment, expect to run the TRITON Unified Installer, the Content Gateway Linux installer, and, if needed, the Web Linux installer. A typical deployment will include at least 4 machines:

1. Use the TRITON Unified Installer or Web Linux Installer to perform a **Custom** installation for core filtering components (Policy Broker, Policy Server, Filtering Service, Network Agent, User Service, Usage Monitor) on a supported Windows or Linux machine.
2. Use the TRITON Unified Installer to perform a **TRITON Manager > Web module** installation to install core management components and reporting tools on a supported Windows machine.

   Installing the TRITON Manager requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 SP2 Express is installed.
3. Use the TRITON Unified Installer to perform a **Custom > TRITON AP-WEB** installation of Log Server on a supported Windows machine.
4. Use the Content Gateway Linux installer to install Content Gateway on a Linux server. No other Websense web protection components can reside on this machine.

Content Gateway

- Content Gateway is installed in **/opt/WCG**, and files are installed with **root** ownership. Content Gateway processes are run as **root**.
- The Content Gateway host computer should have Internet connectivity before you start the installation. Analytic databases cannot be downloaded from the Websense Database Download Server until Internet connectivity is available.
- A full deployment of Content Gateway requires that several ports be open. See Content Gateway Deployment Issues in the Deployment and Installation Center for information about open ports and the reassignment of ports, if necessary.
- The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

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

  - $ (dollar symbol)
  - : (colon)
  - ‘ (backtick; typically shares a key with tilde, ~)
  - \ (backslash)
  - “ (double-quote)
- When Content Gateway and TRITON AP-DATA are deployed together and any of the following file types are used, you must apply Content Gateway v8.0 Hotfix 1. If you do not, files of these types are not detected by Content Gateway.

  - JT Assembly File
  - STL CAD binary format
  - PRO/Engineer Format (.prt)
  - PRO/Engineer Format (.drw)
  - PRO/Engineer Format (.asm)
  - PRO/Engineer Format (.frm)

  To obtain the hotfix, visit MyWebsense.com, select TRITON AP-WEB v8.0, and then select “v8.0.0 HF 01 WCG Failed to Detect AP-DATA File Types”.

TRITON AP-WEB on an appliance

A simple TRITON AP-WEB appliance deployment requires you to:

1. Run the **firstboot** script and configure the full policy source appliance.

   Content Gateway is automatically included on the appliance.
2. Download the TRITON Unified Installer (**WebsenseTRITON80Setup.exe**).
3. Run the installer on a Windows Server 2008 R2, 2008 R2 SP1, 2012, or 2012 R2 machine.
   - Select the TRITON Manager radio button, and the Web module check box beneath it.

   Installing the TRITON Manager requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 SP2 Express is installed.
4. Run the TRITON Unified Installer again (on the TRITON Management Server or another machine) and select **Custom**, then **TRITON AP-WEB** to install off-appliance components that are not part of the TRITON console, like transparent identification agents.

Start-to-finish installation instructions covering most typical deployments are available in PDF format:

- Installation Instructions: TRITON AP-WEB

Downloading the installer

The same installers are used for both fresh installations and upgrades. To download the TRITON Unified Installer, Web Linux Installer, or Content Gateway Installer:

1. Go to mywebsense.com and log in to your account.

   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product** and **Version** (8.0).

   The available installers are listed under the form.
4. Click the plus sign ("+") next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

Note that the TRITON Unified Installer is very large (approximately 1.6 GB), so if you have a slower network connection, it may take some time to download.

> **Note**
> If Content Gateway is running on a V-Series appliance, it is installed during factory imaging and upgraded when the v8.0 patch is applied. You do not need to download the installer.

Upgrade overview

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

See *Downloading the installer* for information on where to get the installation package you need for the upgrade. The same package is used for upgrades as well as fresh installations.

To upgrade to TRITON AP-WEB version 8.0:

- Websense TRITON Web Security Gateway or Web Security Gateway Anywhere deployments must be at version 7.8.x.

  Note that hotfix 94 must be applied to v7.7.x prior to upgrading Content Gateway (software or appliance) to v7.8.x. This retains the default Sync Mode setting between v7.7.x and v7.8.x and then from v7.8.x to v8.0.x. Retaining sync mode can prevent latency sometimes caused by async scanning.
- All components that you want to upgrade (rather than install separately after core components are upgraded) must be on a supported operating system. This may require:
  1. Reinstalling your existing version of Policy Broker and Policy Server on a platform supported in v8.0.
  2. Migrating policy and configuration settings to the new installation on the new platform. (See Migrating web protection management components.)
  3. Running the upgrade process.
- If you are using a version of Microsoft SQL Server prior to 2008, upgrade the database to a certified version.
- When you upgrade Content Gateway from 7.7.x to 7.8.x, in preparation for upgrading to v8.0.x, customized error message pages are lost. Record your customizations in advance and be prepared to reapply them after upgrade.

- If upgrading Content Gateway from a version prior to 7.8.2, if both of the following are true, domain names will be logged after upgrade:

  1. Allow Query Destination has been enabled.
  2. IP addresses are being logged.

  A variable was added and enabled in 7.8.2 that allows domain names to be logged when Allow Query Destination is enabled. (See Reducing DNS Lookups in Content Gateway Manager Help for more information.)
- After upgrading Content Gateway, when TRITON AP-DATA is on the same machine, a reboot may be required to deploy Data policies.
- When Content Gateway and TRITON AP-DATA are deployed together and any of the following file types are used, you must apply Content Gateway v8.0 Hotfix 1 after the upgrade is complete. If you do not, files of these types are not detected by Content Gateway.

  - JT Assembly File
  - STL CAD binary format
  - PRO/Engineer Format (.prt)
  - PRO/Engineer Format (.drw)
  - PRO/Engineer Format (.asm)
  - PRO/Engineer Format (.frm)

  To obtain the hotfix, visit MyWebsense.com, select TRITON AP-WEB v8.0,and then select “v8.0.0 HF 01 WCG Failed to Detect AP-DATA File Types”.

Once all components are on a supported platform and a supported database engine is in place, upgrade your components in the following order:

1. Upgrade the Policy Broker machine (or full policy source appliance). If upgrading from 7.8.1 or later, this would be the primary (or standalone) Policy Broker machine.
2. If upgrading from 7.8.1 or later, upgrade any replica Policy Broker machines you may have.
3. Upgrade any Policy Server machines that do not have a Policy Broker installed.
4. Upgrade the Log Server machine (if different from the Policy Broker or Policy Server machine).

   To support reporting on IPv6 addresses, upgrading from a version prior to 7.8.4 will create a new logging partition in the Log Database.
5. Upgrade the TRITON management server (if on a separate machine from Policy Broker, Policy Server, or Log Server).
6. Upgrade any user directory and filtering appliances. If you have multiple user directory and filtering appliances, the upgrade processes can run in parallel.
7. Upgrade any filtering only appliances. If you have multiple filtering only appliances, the upgrade processes can run in parallel. (Be sure that all Policy Server instances, on and off appliance, have been upgraded before you upgrade filtering only appliances.)
8. Upgrade all other machines hosting web security software. The upgrade processes for multiple machines can run in parallel.
9. Upgrade any endpoint client software on end user machines (if used).

Installation and upgrade tools and references

- Deployment and Installation Center: Web Protection Installation
- Deployment and Installation Center: Web Protection Upgrade
- Websense Default Ports

Operating tips

Topic 51123 | Release Notes | TRITON AP-WEB | 02-Feb-2015

Working in the TRITON Manager

To improve your experience with the Web module of the TRITON Manager:

- Disable all browser pop-up blocking features.
- If you have problems accessing the console from Internet Explorer:
  1. Make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
  2. If problems continue, reset Internet Explorer to its default configuration. To do this, in Internet Explorer, go to **Tools > Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.
- If this is your first experience with a Websense web protection solution, review the New Admin Quick Start tutorial (Help > Getting Started > New Admin Tutorial) for help getting started with policy management and reporting.
- Avoid using the browser Back and Refresh buttons. Instead, use the breadcrumbs at the top of the page or the left and right navigation panes.
- **Click OK at the bottom of each page in the Web module of the TRITON Manager to cache changes made on the page.**

  In some instances, when you are performing secondary tasks, you must click OK on the secondary page, and then click OK again on the main page to cache your changes. Make sure you see the “Changes have been cached” success message.
- Click **Save and Deploy** to implement cached changes.

  It can take up to 30 seconds for all Websense components to be updated with the changes.

Using reporting tools

To improve your experience with your reporting tools:

- If you install TRITON management components first, and then install Log Server, manually restart the **Websense TRITON - Web Security** service on the TRITON management server machine. This ensures that reporting data appears in the Web module of the TRITON Manager, and that presentation reports scheduled jobs are properly stored in the Log Database.

- If you are using Internet Explorer 8, make sure that Compatibility View (the button between the URL and the Refresh button in the browser address bar) is turned **off**.

Content Gateway

The following details are provided to help improve your experience with Content Gateway.

Installation

- Content Gateway tolerates different software versions in the same cluster. This is intended to simplify the process of upgrading a cluster. You should not run a cluster containing different versions for a prolonged period of time (many days).
  - Configuration synchronization does **not** take place among nodes of different versions.
  - Condition alarms are passed among all nodes.
  - The VIP feature is supported.
- 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.

Configuration

In explicit proxy deployments, send HTTPS traffic to port 8080

In explicit proxy deployments, when HTTPS (SSL support) is enabled, client browsers should be configured to send HTTPS traffic to proxy port 8080.

Accessing Intranet sites in an explicit proxy deployment

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.example.com
```

For external websites:

```
nslookup www.example.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”.

DNS proxy caching

The DNS proxy caching option allows Content Gateway to resolve DNS requests on behalf of clients. This option off-loads remote DNS servers and reduces response times for DNS lookups. You can use the DNS proxy caching option only with a layer 4 switch or a Cisco router running WCCP v2.

DNS proxy caching can only answer requests for A and CNAME DNS entries. Other types of request (e.g., MX) will not be answered.

Limitation: If the host name to IP address mapping is not in the DNS cache, Content Gateway contacts the DNS server specified in the **/etc/resolv.conf** file. **Only the first entry in resolv.conf is used.** This might not be the same DNS server for which the DNS request was originally intended.

See “DNS Proxy Caching” in Content Gateway Manager Help.

If your environment is configured such that you have DNS servers that resolve internal sites only and others that resolve external sites only, see Using the Split DNS option in Content Gateway Manager Help.

Using extended event logging

To investigate unexpected system behavior, it is sometimes helpful to enable the **Log Transaction and Errors** option (extended event logging) in Content Gateway Manager (**Configure > Subsystems > Logging**). However, extended event logging adds significant load to Content Gateway processes. Therefore you should **not** enable extended event logging when Content Gateway is at the high end of its processing capacity.

Reverse proxy

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

IWA support for load balanced environments

Important

After upgrade to v8.0.0 check and, if necessary, rejoin IWA domains.

If you customized your 7.8.2 or higher deployment to support an external load balancer with IWA user authentication (see the description, below), the configuration is preserved during upgrade to version 8.0.x. You do not need to re-apply the custom configuration. You should, however, test your deployment to verify that the load balancer is performing as expected.

With Websense Content Gateway, Integrated Windows Authentication (IWA) uses the Kerberos protocol, with NTLM fallback.

In an explicit proxy deployment with an external load balancer, because the clients point to a FQDN that does not match the Content Gateway hostname, they receive a Kerberos ticket that Content Gateway cannot decrypt.

Normally, Content Gateway would be configured to share the hostname of the load balancer, but this is not possible when the load balancer requires hostname resolution (as with DNS-based load balancing).

In these cases, Content Gateway must be configured to use a custom keytab that corresponds to the load balancer's hostname for decryption.

Samba's implementation of Kerberos prevents this, because it requires keytab entries to match the service's hostname.

Please see Configuring Integrated Windows Authentication with a load balancer in Content Gateway manager Help for more information.

Proxy user authentication

Client browser limitations

Not all Web browsers fully support transparent user authentication (prompt-less).

The following table indicates how a browser responds to an authentication request when Integrated Windows Authentication (IWA) is configured.

Browser/ Operating System	Internet Explorer (v10, 11 tested)	Firefox	Chrome	Opera	Safari
Windows	Performs transparent authentication	Performs transparent authentication (v28, 32 tested)	Performs transparent authentication (v34, 35, 38 tested)	Performs transparent authentication (v24 tested)	Falls back to NTLM and prompts for credentials (v5.34.57 tested)
Mac OS X	Not applicable	Performs transparent authentication (v28, 32 tested)	Falls back to NTLM and prompts for credentials (v38 tested)	Falls back to NTLM and prompts for credentials(v20 tested)	Performs transparent authentication (v7.0.2 tested)
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication (v28 tested)	Browser issue prevents IWA from working (v34,35 tested)	Not tested	Not applicable

SSL Internal Root CA

It is strongly recommended that all instances of Content Gateway use the same Root CA, and that for best security the signature algorithm be SHA-2, although SHA-1 is supported.

The default Root CA (presented to clients) is signed with SHA-256.

The best practice is to replace the Websense default Root CA with your organization's Root CA signed by SHA-2 or stronger. See Internal Root CA in Content Gateway Help.

The Root CA should be imported into all affected clients.

Note

Client connections may fail (depending on specific browser behavior) if the client sees a certificate generated by an unknown Root CA.

Resolved and known issues

Topic 51124 | Release Notes | TRITON AP-WEB | 02-Feb-2015

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

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