websense

SSL Manager Certificate Verification Engine

Websense Content Gateway

v7.6.2

Websense Content Gateway SSL Manager Certificate Verification Engine

February, 2012

R033011760

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., and Yahoo, Inc. make no warranties with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Portions of Websense Content Gateway include third-party technology used under license. Notices and attribution are included elsewhere in this manual.

1 SSL Manager Certificate Verification Engine v7.6.2

The Websense® Web Security Gateway proxy component – Content Gateway – includes a feature called SSL Manager. SSL Manager oversees SSL and TLS (HTTPS) connections, decryption, analysis of content, and re-encryption.

This article describes the most effective use of the Certificate Verification Engine, a sub-component of SSL Manager. The Certificate Verification Engine ensures that only those connections that comply with your organization's IT security requirements for certificate verification are allowed.

This guide includes:

- *Overview*
- *SSL Manager Certificate Verification Engine (CVE)*
- *CVE Best Practices*
- *Certificate Verification Failures and Remediation Options*
- *Troubleshooting* Certificate Verification Failures
- *Frequently Asked Questions*
- *Known Issues*
- *Additional Resources*
- *Glossary*

For general information on SSL Manager, see Working with Encrypted Data in the Websense Technical Library. (Several articles follow in a sequence. Use the right-pointing navigation button at the top and bottom of each article.)

Overview

The SSL and TLS protocols used by HTTPS Web traffic are the standard for establishing secure connections and transmission of secure data on the Internet.

Although SSL and TLS are considered strong security protocols, if mismanaged HTTPS can be compromised in ways that leave it vulnerable to many of the same security problems found in standard HTTP traffic.

An essential feature of SSL/TLS is the connection handshake, including digital certificate exchange between the client and server that verifies that each agent is who it says it is.

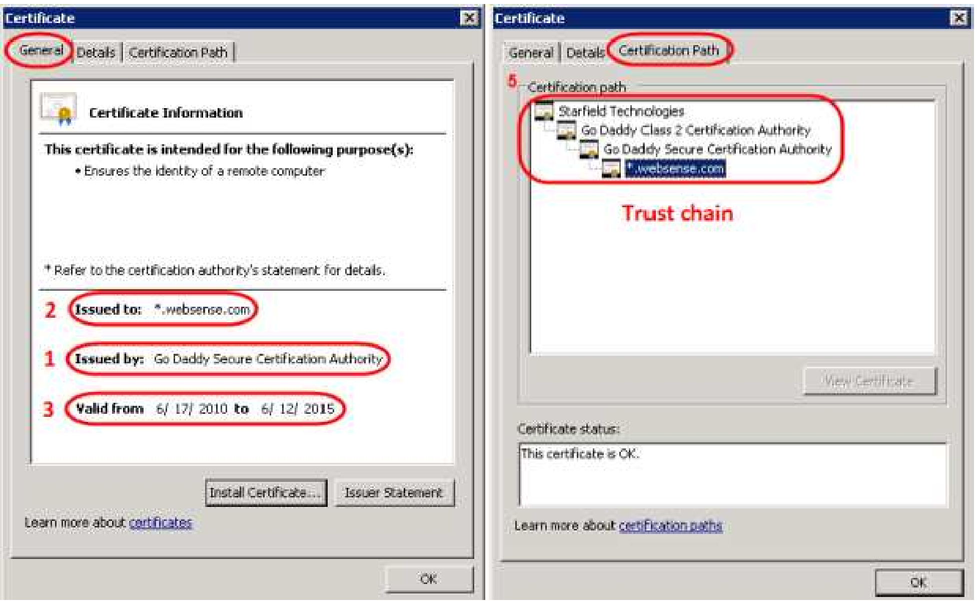
Verification checks are performed and configurable in Content Gateway.

In the following list, quoted field names (“ ”) are those used by Internet Explorer Version 8 (IE8).

Common verification checks include:

1. The certificate must be issued by a trusted Certificate Authority (CA).
2. The fully qualified hostname in the HTTPS request URL and the certificate owner (“Issued to” name) must match. Exceptions are explained in the *SSL Manager Certificate Verification Engine (CVE)* section.
3. The certificate must be current (within its “Valid from...to...” date range).
4. The certificate must not be on a revocation list (either CRL or OCSP).
5. Checks 1-4 are recursively applied to every certificate in the trust chain.

Below is a certificate as it appears in IE8. The numbers in red correspond to checks in the preceding list.



Certificate
General | Details | Certification Path
Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

2 Issued to: *.websense.com

1 Issued by: Go Daddy Secure Certification Authority

3 Valid from 6/ 17/ 2010 to 6/ 12/ 2015

Install Certificate...
Issuer Statement
Learn more about certificates
OK
Certificate
General | Details | Certification Path
5 Certification path
Starfield Technologies
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
*.websense.com
Trust chain
View Certificate

Certificate status:

This certificate is OK.

Learn more about certification paths
OK

When the handshake is successful, a secure connection is established and encrypted content is passed.

SSL Manager Certificate Verification Engine (CVE)

Prior to establishing an HTTPS connection, it is the job of the Certificate Verification Engine to verify that the Certificate Authority (CA) certificates offered by destination HTTPS servers are legitimate and meet the configured set of verification conditions.

To turn on the CVE:

Enable the certificate verification engine

Verification options:

Deny Certificates where the common name does not match the URL

Allow wildcard certificates

No expired or not yet valid certificates (default option)

Verify entire certificate chain (default option)

Check certification revocation by CRL (default option)

Check certification revocation by OCSP

Preferred method for revocation check

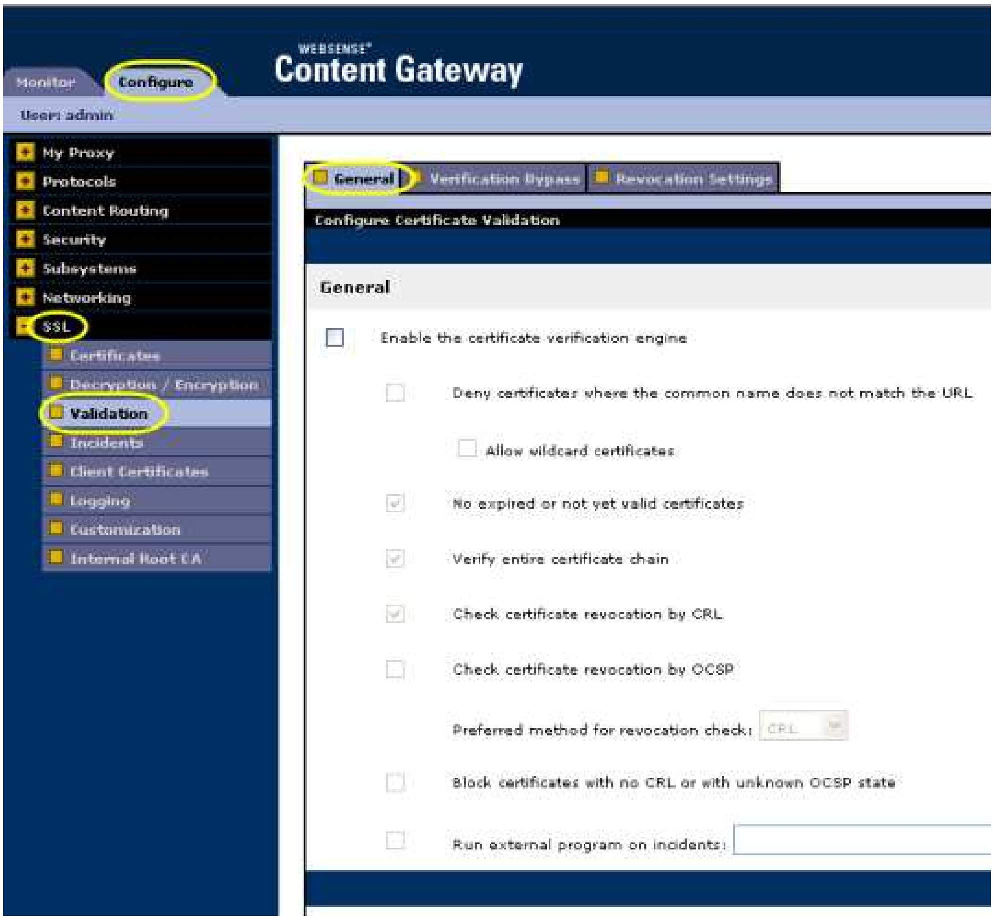
Block certificates with no CRL or with unknown OCSP state

CVE options

For Help system documentation on the CVE, see Validating certificates.

Configuration options are set in Content Gateway Manager on the **Configure** > **SSL** > **Validation** > **General** page. The illustration below shows the page with the default settings.

> **Important**
> Understanding the behavior of each option is the best way to achieve your certificate verification objectives.



Configure Certificate Validation

General

☐ Enable the certificate verification engine

☐ Deny certificates where the common name does not match the URL

☐ Allow wildcard certificates

☑ No expired or not yet valid certificates

☑ Verify entire certificate chain

☑ Check certificate revocation by CRL

☐ Check certificate revocation by OCSP

Preferred method for revocation check: CRL

☐ Block certificates with no CRL or with unknown OCSP state

☐ Run external program on incidents:

Option	Description
Enable the certificate verification engine	Enables the CVE. The CVE is **disabled** by default. This prevents the Content Gateway administrator and network users from being taken by surprise by the effects of certificate verification when HTTPS is initially enabled (on the **Configuration** > **My Proxy** > **Basics** page).
Deny Certificates where the common name does not match the URL	When enabled, a certificate with a Common Name that does not exactly match the fully qualified domain name in the destination URL results in a verification failure. The check also attempts a match for Subject Alternative Name (SAN). The check ignores case. Because an exact match is required, there may be instances when a legitimate variation in the Common Name, or the absence of a matching variation in the SAN, may result in a block. For example, using “https://cia.gov” when attempting to access “https://www.cia.gov” may result in a block. Additionally, a block may occur when a user is accessing a Web site by IP address.

Option	Description
Allow wildcard certificates	When **Deny Certificates where the common name does not match the URL** is enabled, use this option to allow matches with Common Names that include the "*" (wildcard) character in the name. Some HTTPS servers use a certificate with a wildcard in the name so that a single certificate can cover an entire domain. For example: "*.example.com" to cover "email.example.com" and "stream.example.com", and so forth. Use of the wildcard means that individual servers within the domain are not verified; they are included as a result of the wildcard. Allowing wildcard certificates eases the strict matching burden when a Common Name match is required. It is also helpful for domains that have multiple subdomains like google.com or yahoo.com. However, it also creates the risk of fraudulent or undesirable variations of a domain remaining unblocked. **Note: This check is case-sensitive in all Content Gateway versions up to and including 7.6.2.** The check will be changed to ignore case in a future release.
No expired or not yet valid certificates (default option)	Denies access to sites whose certificates are expired or not yet valid. This is a basic check that is very important because many malicious sites operate with expired certificates. If this option is not selected, access to those sites is permitted. **Note:** Self-signed certificates (certificates without an official CA) are considered invalid and belong in this category.
Verify entire certificate chain (default option)	Verifies expiration and revocation status of all certificates between a certificate and its root Certificate Authority as specified in the Certification Path of the certificate.
Check certification revocation by CRL (default option)	Certificate revocation lists (CRLs) are used to check a certificate's revocation status. CRLs list certificates that have been issued and subsequently revoked by the CA. Verifying the revocation status is a basic check and is very important because certificates are typically revoked when they are improperly issued, have been compromised, have a false identity, or violate policies specified by the CA.
Check certification revocation by OCSP	The Online Certificate Status Protocol (OCSP) is an alternate way to check a certificate's revocation status. While OCSP is beneficial, it is not as widely used as CRLs and, therefore, is not as reliable. Also, it is a real-time, Internet-hosted check that can introduce request handling latency.
Preferred method for revocation check	When both CRL and OCSP revocation checking are enabled, you can select which method to apply first. The default is CRL. **IMPORTANT:** This option has no effect in version 7.6.0 or 7.6.2. CRL checking is always performed first. The problem will be corrected in a future release.
Block certificates with no CRL or with unknown OCSP state	This option blocks sites that offer certificates for which the revocation status cannot be determined, including OCSP status "unknown". Because many certificates do not include CRL or OCSP information, this option can result in a high number of verification failures. Often the failures are reported as "Unknown revocation state" errors. You can view certificate CRL and OCSP information in a browser by choosing to view the certificate.

CVE Best Practices

In the management of HTTPS traffic, verification of the CA-issued digital certificates is very important to security.

Skipping certificate verification significantly weakens HTTPS security and the security of your network.

However, certificate verification is not free of risk.

- Certificate checks fail in expected and intended ways when browsing to sites with certificates authorities not known to the Websense Content Gateway. That's security. Regular, proactive user education helps users recognize legitimate failures and prevents Helpdesk phones from ringing unnecessarily. See *Frequently Asked Questions* for a summary of information for users.
- *Certificate checks also fail in unexpected and unintended ways* that also require user education, as well as administrative effort in the form of investigation and remediation.

Therefore, when using SSL certificate verification, you need to know:

- Your organization's certificate verification requirements as they pertain to your IT security policy.
- Your organization's ability and willingness to manage the administrative burden. When verification fails and there is no remediation in place, the connection request is dropped and users often call Helpdesk. Some number of failures will require administrator investigation and remediation.

To administer certificate verification, you need to:

- Know which failures legitimately protect your network
- Know how to investigate failures
- Determine which failures are undesirable and can be remediated (certificate replacement, verification bypass, other)
- Educate users about SSL connection failures; what they look like; why they occur
- Anticipate more Helpdesk calls

Important

It is recommended that you **not** use Content Gateway to proxy internal traffic.

However, if you do, before enabling the CVE audit, your internal HTTPS servers to ensure that their certificates are valid and trusted by SSL Manager.

If you plan to use the CVE, be sure to acquaint yourself with these topics:

- *Troubleshooting* certificate verification failures
- *Certificate Verification Failures and Remediation Options*
- SSL transaction logging

CVE configurations

This section describes a phased approach to deploying certificate verification.

It is recommended that in addition to the production environment, Content Gateway be installed in a controlled test environment in which phased configuration can be tested and monitored, and problems remediated and tested again. When the test environment is functioning as desired, the configuration can be rolled out to the production environment with continued monitoring and testing.

The starting point assumes that Content Gateway is stable and SSL Manager is off.

The phases of SSL Manager and CVE deployment include:

1. Enabling SSL Manager.
2. Enabling the CVE with only the certificate revocation (CRL) check enabled.
3. Adding CVE checks to the configuration as needed.

Enabling SSL Manager

Before enabling SSL Manager, verify that Content Gateway:

- Is installed in a supported environment that includes a network test segment
- Is passing explicit or transparent traffic as expected
- Is integrated with Web Security, including Scanning options set and policy applied as expected
- Is handling HTTP traffic as expected
- Is stable:
    - The performance monitoring graphs show a predictable ramp up in traffic with no unexplained traffic spikes
    - All mission critical Web sites and Web-hosted applications have been validated to work properly through the proxy

When the above conditions are met:

- Enable SSL Manager.
- Confirm that HTTPS traffic is passing through Content Gateway.
- Verify that clients are not receiving certificate errors in the browser. If they are, see these instructions on installing the Internal Root CA.
- Test by accessing several sites that are commonly used in your organization.

- Test by using HTTPS-based applications that are commonly used in your organization. See these articles for information about common problems.
    - Dropped HTTPS connections
    - Web sites that have difficulty transiting Content Gateway
- Send a representative sample of traffic into the test environment with the objective of uncovering as many HTTPS traffic problems as possible.
- When the environment is stable, proceed to enabling the CVE with the CRL check.

Enabling the CVE with only the CRL check enabled

Now that SSL Manager is on and stable, enable the CVE with just CRL checking enabled.

This is the recommended second step because the CRL check is an essential certificate verification check that rarely fails in error.

Repeat the testing performed after enabling SSL Manager.

If a certificate fails because it is on a revocation list, a fast and easy way to confirm the revocation status is to use a Web-hosted certificate verification tool. Using a browser and a common Search site, search for “SSL checker”. Select a site that you trust and enter the exact URL of the site that failed.

At this stage, to minimize disruption to users, you may also want to enable Verification Bypass. See *CVE with Verification Bypass enabled*.

Adding CVE checks to the configuration

When you are satisfied with certificate verification using only the CRL check, if you want to enable additional options it is recommended that you enable them one at a time, repeating the testing regiment established in the first phase.

These are the three default checks in version 7.6. If you are following the recommended steps, “Check certificate revocation by CRL” is already enabled.

- *No expired or not yet valid certificates (default option)*
- *Verify entire certificate chain (default option)*
- *Check certification revocation by CRL (default option)*

For each option enabled, when there is a certificate verification failure, an incident is added to the Incident List. Begin troubleshooting by examining the Incident List. See *Troubleshooting*.

The remaining CVE options are:

- *Deny Certificates where the common name does not match the URL* and its child *Allow wildcard certificates*

  Unfortunately, Common Name mismatches are common and produce a variety of error messages (see *Troubleshooting*). Enable this option first in the test environment and perform ample testing.

- *Check certification revocation by OCSP*
- *Preferred method for revocation check*

  In version 7.6.0 and 7.6.2, this option has no effect. The CRL check is always performed first.
- *Block certificates with no CRL or with unknown OCSP state*

  Because many certificates have missing or blank CRL or OCSP information, this option can produce a large number of "Unknown revocation state" errors. For this reason, use of this option is **not** recommended in versions up to and including 7.6.2. The CVE logic for this option will change in a future release.

CVE with Verification Bypass enabled

An additional option includes use of SSL Manager Verification Bypass (**Configure** > **SSL** > **Validation** > **Verification Bypass**). This option has the effect that when certificate verification fails, a dialog box warns the user of the failure and gives the user the option to go to the site anyway.

Advantages include:

- Certificate verification is performed and incidents are logged, but users aren't blocked. Users are allowed to make the decision about whether a site is safe.
- Administrators can see how the CVE affects the network before allowing it to impact users or require an administrator response.
- By monitoring the Incident List, administrators can put remediation actions in place before enforcing certificate verification and impacting users.
- Verification bypass provides a response to users that is much like the warning dialogs used by common browsers.

Disadvantages include:

- Security is compromised because the choice to drop the connection is given to the user.
- In cases where the HTTPS request is for an object embedded in the page or in another page, and its certificate verification fails, the bypass page may not render.

Best practices summary

- After Content Gateway is deployed, quickly identify and resolve Web applications that have problems transiting the proxy.
- Work in a test environment.
- Turn on SSL Manager, monitor, test, and stabilize.
- Turn on CVE checks one at a time, test, monitor, remediate, and retest.
- Roll out the configuration to a subset of users.
- To reduce administrative overhead, do not enable checks that aren't required by your IT security policy.

Certificate Verification Failures and Remediation Options

When certificate verification fails, an access denied message is displayed to the user and an incident is entered in the SSL Manager Incident List.

If the CVE blocks access to a site believed to be safe, the administrator should research the failure in the Incident List, and may want to research the status of the destination host.

Certificate verification failures occur for the following reasons:

Important
The failures that you see at your site will depend, in part, on the CVE options you have enabled.

1. An invalid or mishandled SSL handshake (e.g., Skype, Citrix GoTo services)
2. A certificate that was not issued by a CA in Content Gateway's trusted CA list; this is often a self-signed certificate
3. A certificate that was not issued by a CA that is trusted by the destination server
4. A revoked CA (on a CRL or OCSP list)
5. An expired or not yet valid certificate
6. An expired, not yet valid, or revoked certificate in the certificate chain
7. A name mismatch between the hostname and URL, or similar (hostname and the Common Name, hostname and the Subject Alternative Name; hostname and use of a wildcard in the certificate)
8. Missing and/or optional fields in the certificate (no CRL or OCSP state; result in "Unknown revocation state" errors)
9. A problem in the logic of the CVE

List of common certificate verification error messages

See the *Troubleshooting* certificate verification failures section for more information on each of these errors.

1. CA explicitly denied
2. Certificate has expired
3. Certificate is not yet valid
4. Certificate revoked
5. Client certificate requested
6. Common Name does not match URL
7. Invalid CA certificate
8. Self-signed certificate

9. Self-signed certificate in certificate chain
10. Unable to get local issuer certificate
11. Unable to verify the first certificate
12. Unknown revocation state

Remediation

Certificate verification failures can be remediated in several ways.

Important

The SSL Manager Incident List is the primary vehicle for investigating verification failures. To effectively use the CVE, administrators must become fluent with the SSL Manager Incident List facility. Help system information starts here.

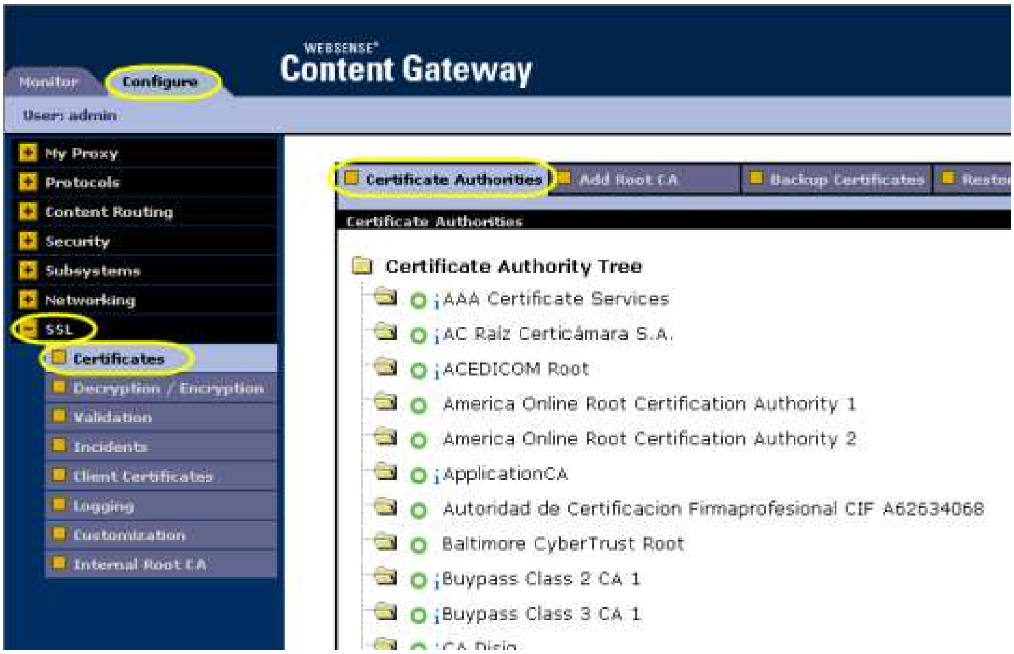
The primary remediation options include:

1. Correcting the certificate problem. See *Troubleshooting* certificate verification failures and the *SSL Manager trusted certificate store*.
2. Bypassing certificate verification via SSL Decryption bypass, the SSL Manager Incident List, or another bypass option. See *Bypass options.*
3. Enabling or disabling *CVE options*.
4. Using the **CVE Verification Bypass** option to give users the ability to proceed to a site after certificate verification fails.

SSL Manager trusted certificate store

When version 7.6 of Content Gateway is installed, all Certificate Authorities trusted by Internet Explorer 7 are included in the SSL Manager trusted certificate store.

The list is accessed in Content Gateway Manager on the **Configure** > **SSL** > **Certificates** > **Certificate Authorities** tab.



Certificate Authority Tree

- ¡AAA Certificate Services
- ¡AC Raíz Certicámara S.A.
- ¡ACEDICOM Root
- America Online Root Certification Authority 1
- America Online Root Certification Authority 2
- ¡ApplicationCA
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- Baltimore CyberTrust Root
- ¡Buypass Class 2 CA 1
- ¡Buypass Class 3 CA 1
- ¡CA Disig

Destination servers (the target of outbound traffic from SSL Manager) can trust Web servers with these certificates. Note that lowercase "i" appears before the name of some certificates validated via CRL (certificate revocation lists) or OCSP (online certification status protocol). These certificates provide URLs where their revocation status can be verified. See Keeping revocation information up to date.

You can manually add, delete, or change the status of a certificate.

SSL Manager checks the revocation status of a certificate for both inbound and outbound traffic.

Help system information on SSL Manager certificate management starts here.

SSL transaction logging

SSL Transaction logging is described here.

Bypass options

Bypass is the term used to describe several methods of specifically allowing a request to circumvent (bypass) all or select features of Content Gateway. Full proxy bypass is often called tunneling.

In this discussion take note of when bypass affects:

- Only certificate verification
- Certificate verification and SSL decryption
- Complete bypass of Content Gateway

These are the primary bypass methods:

- TRITON – Web Security SSL decryption bypass (category and destination hostname/IP address)
- The Content Gateway SSL Manager Incident List
- Content Gateway ARM bypass (transparent proxy)
- Explicit proxy PAC file bypass
- Transparent proxy routing device ACL bypass
- Allow users to continue after failure (**Configure** > **SSL** > **Validation** > **Verification Bypass**)

TRITON – Web Security SSL Decryption Category bypass and Hostname/IP address bypass

In **TRITON – Web Security** you can specify categories, or hostnames, or IP addresses of Web sites for which SSL decryption and inspection are not performed. See SSL Decryption Bypass.

If Content Gateway is set up as an **explicit proxy**, certificate verification **is bypassed**, leaving certificate verification subject to the settings of the client browser. This is the best practice for bypass in explicit proxy deployments.

If Content Gateway is set up as a **transparent proxy**, certificate verification **is not bypassed**. In transparent proxy deployments, Content Gateway first retrieves the site certificate, performs validation, and then uses the Common Name to determine if SSL Decryption Category bypass or Hostname/IP address bypass is performed. Therefore, in transparent proxy deployments, the Content Gateway Incident List is the best way to set up bypassing for specific sites.

SSL Manager Incident List

The SSL Manager Incident List is the principal SSL decryption and certificate verification bypass mechanism in Content Gateway. In addition to automatically adding certificate verification failures (incidents) to the list, administrators can manually add destination URLs.

Administrators should set “Action:Allow” to bypass certificate verification (the check is made but has no effect). Administrators should use “Action:Tunnel” to bypass certificate verification and SSL decryption. See Managing Web HTTPS site access.

Content Gateway ARM bypass

See Interception bypass.

Explicit proxy PAC file bypass

See:

- How do I specify in a PAC file a URL that will bypass Content Gateway?
- PAC File Best Practices

Transparent proxy Access Control List (ACL) bypass

See the vendor documentation for your transparent routing device.

SSL Manager Verification Bypass

See SSL Manager Verification bypass.

Troubleshooting

This section describes how to use resources in Content Gateway and on your PC to troubleshoot certificate verification failures.

As new information becomes available, updated Troubleshooting information will be posted online to Troubleshooting for Certificate Verification.

✓ **Note**

Several Web sites offer excellent online SSL checkers that diagnose problems with SSL certificates installed on Web servers. To access one of those tools, in a browser go to a Search service and search for "SSL checker".

When a failure occurs:

1. Note the incident ID and URL in the block page displayed to the user.
2. Log on to Content Gateway Manager and go to **Configure** > **SSL** > **Incidents** > **Incidents List**.
3. Search for the incident ID and verify the URL.
4. In the Message field, click the magnifying glass to view the complete details. It is important to note the "depth=" value because it indicates the location within the chain where the error occurred.

If the message is:

Message	Description & Action
Certificate is not yet valid	The certificate's "Valid from" date is in the future. Verify the failure by accessing the same URL without Content Gateway and check the "Valid from ---- to ----" fields. The "Valid from" date should be a date in the future. If the **Verify entire certificate chain** option is enabled, the "Valid from" date of every certificate in the chain may have to be checked. Look for the "depth=" value in the error message for the level in the chain at which the error occurred. **Note:** Also check that the time and date are set correctly on the Content Gateway host system. To check the time in Content Gateway Manager, go to **Monitor** > **My Proxy** > **Alarms**.
Certificate has expired	The certificate's "Valid to" date is in the past. Verify the failure by accessing the same URL without Content Gateway and check the "Valid from ---- to ----" fields. The "Valid to" field should be a date in the past. If the **Verify entire certificate chain** option is enabled, the expiration date of every certificate in the chain may have to be checked. Look for the "depth=" value in the error message for the level in the chain at which the error occurred.

Message	Description & Action
Self-signed certificate	The offered certificate is self-signed and the same certificate cannot be found in the list of trusted certificates. Verify the failure by accessing the same URL without Content Gateway. The browser should get the same error.
Self-signed certificate in certificate chain	The certificate chain cannot be built up due to an untrusted self-signed certificate, or the root CA is not yet added to the CA tree. To verify if the failure is due to an untrusted self-signed certificate in the chain, access the URL without Content Gateway to produce the same error. When a certificate is signed by its own issuer, it is assumed to be the root CA. Verify if the root CA is listed on the CA tree by going to **Configure > SSL > Certificates.** **Note:** This is a common error, especially with network equipment that includes HTTPS management interfaces. If the devices are internal to your network, you may want to bypass proxying altogether. To resolve this issue, you would have to import a certificate from a trusted source, or specifically configure SSL Manager to trust the specific certificate.
Unable to get local issuer certificate	The issuer certificate of an untrusted certificate cannot be found. When this failure occurs, the error message displays “depth= 0”, which indicates that the problem is the peer or local issuer certificate. A trusted CA certificate (depth= 1) is required. Investigate the problem by accessing the site without Content Gateway and view the certificate in the browser. To identify the certificate from the Certification Path that does not appear in the CA tree, look up one level in the chain. Then, compare the identified certificate to the CA tree to verify the missing certificate (**Configure > SSL > Certificates**). Make a copy of the missing certificate and add it to the trusted certificate tree. See *How do I copy a certificate from my browser to the CA tree?*. Remove the incident from the Incident List and then access the site again to confirm that the failure is cleared.
Unable to verify the first certificate	The certificate could not be verified because the Certification Path (certificate chain) contains only one certificate and it is not self-signed. To verify the failure, access the site without Content Gateway, examine the certificate, and verify that the Certification Path includes only 1 certificate and that it is not self-signed. The root CA that signed the certificate must be part of the chain to avert this error.
Certificate revoked	The certificate has been revoked. This is a serious security alert. SSL manager has learned via the CRL or OCSP that the Certificate Authority that signed the certificate has revoked the certificate. A Web search can lead to good information about why the certificate was revoked. To verify the failure, access the site without Content Gateway. The browser should encounter the same error. Also, submit the URL to a Web-hosted SSL certificate checking tool.
Invalid CA certificate	The certificate is invalid. Either the certificate is not a CA or its extensions are not consistent with the supplied purpose.

Message	Description & Action
Common Name does not match URL	The Common Name of the certificate does not match the specified URL. Due to the way that certificates are constructed and URLs specified, this can be a common error. To verify the failure, access the site without Content Gateway, open the certificate, and verify that the Common Name or Subject Alternative Name, if present, does not match the fully qualified hostname in the URL. If your IT security policy permits it, it may work best to configure Verification Bypass to allow your users to bypass the warning at their discretion. Web Security Gateway has additional protections to detect if Web sites are being impersonated. The SSL Manager Verification Bypass feature only allows the user to continue to the site. Web Security is not bypassed by this feature.
Unknown revocation state	A common error when OCSP verification is enabled. To verify the failure, access the site with an OCSP-supported browser and without Content Gateway. The error should occur.
CA explicitly denied	A new CA was added to the CA tree, but is explicitly denied by Content Gateway. To verify and remediate the condition, log on to Content Gateway Manager and go to **Configure** > **SSL** > **Certificates** > **Certificates Authorities**. The new CA should be listed with a red cross to the left. This CA was offered as part of the SSL handshake and added to the CA tree with the status: untrusted. After validating the CA with Content Gateway, set the allow or deny status. From the **Certificate Authorities** page, select the CA to view the deny and allow options. If you elect to allow the CA, delete the incident and go to the site to verify access.
Client certificate requested	The destination server requires a client certificate. To verify the failure, access the site without Content Gateway and confirm that the origin server is requesting a client certificate. **Note:** When a client certificate is required, there is an option to bypass the client certificate. The default bypass option is to create an incident by going to the **SSL** > **Client Certificates** > **General page**.

Frequently Asked Questions

- *Why is the CVE turned off by default?*
- *Why am I getting so many incidents?*
- *How do I know which certificate verification failures are problems that need a response?*
- *What are the best troubleshooting techniques for certificate verification failures?*
- *How do I view a certificate in my browser?*
- *How can I make best use of the Incident List?*
- *Why do some HTTPS sites not load properly?*
- *What causes 'Peer sudden disconnect' errors?*
- *What do my users need to know about HTTPS certificate verification?*
- *How do I copy a certificate from my browser to the CA tree?*
- *How do I check and update a CRL link?*

Why is the CVE turned off by default?

It's off because certificate verification can have a large impact on users and administrators. Educating users and administrators, and preparing the network, are the best practice prior to enabling the CVE. To become familiar with SSL Manager and the CVE, see this section of Content Gateway Manager Help.

Why am I getting so many incidents?

The answer requires analysis of the SSL Manager Incident List. See *Troubleshooting* certificate verification failures. Take into consideration that some CVE options can generate a significant number of incidents, such as *Block certificates with no CRL or with unknown OCSP state*.

How do I know which certificate verification failures are problems that need a response?

You need to become familiar with all of the types of failures that can occur and their causes. See *Troubleshooting* certificate verification failures. For every failure, give consideration to the possibility that the verification check was performed correctly, and that the failure is legitimate. See *CVE options* for a description of each CVE option, the conditions for failure, and the conditions that result in false-positives, if any. Should a failure be deemed an error, or the destination server be deemed safe or necessary, see *Certificate Verification Failures and Remediation Options* for a list of remediation alternatives.

What are the best troubleshooting techniques for certificate verification failures?

See *Troubleshooting* certificate verification failures.

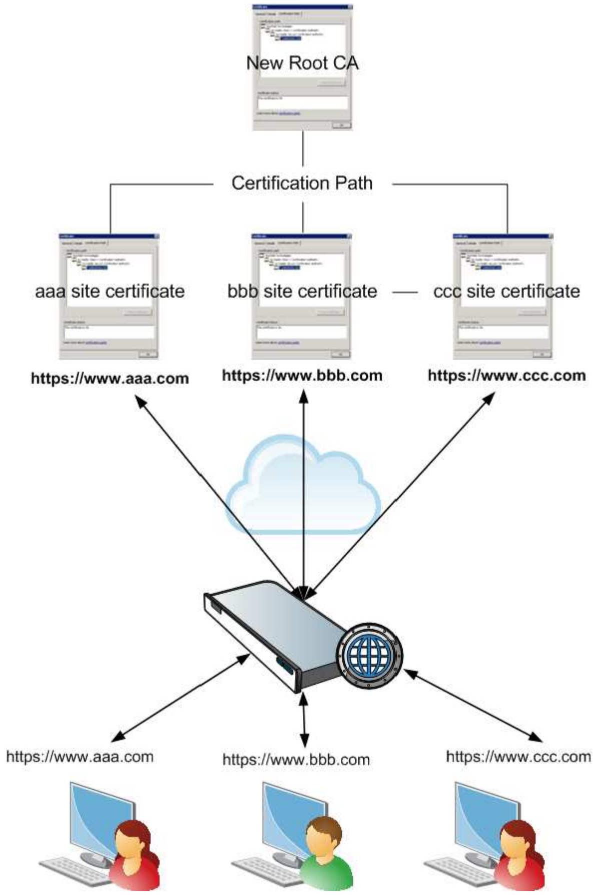
How do I view a certificate in my browser?

In IE8, on the tool bar click **File** and select **Properties**. Then, click **Certificates**.

In Mozilla Firefox, on the tool bar click **Tools** and select **Page Info**. Toggle to the **Security** tab, then click **View Certificate**.

How can I make best use of the Incident List?

1. Review the section in this paper titled *SSL Manager Incident List*. Follow the link to *Managing Web HTTPS site access* to review information for administrators in the Content Gateway Help system.
2. The number of incidents automatically created by certificate verification failures depends on the CVE options enabled and peculiarities of the sites your users visit. For more about CVE options, see *CVE options*.
3. If you have multiple Content Gateway servers in a cluster, configure SSL Manager clustering so that you have only one Incident List to manage. See Clusters.
4. If you have several individual sites on the Incident list and some of those sites have certificates signed by the same new root CA, you could trust the CA that they have in common and delete the individual site entries, thus keeping the Incident List as small as possible.



5. Do **not** add “*.*” as “Action:Tunnel”. This has the effect of tunneling all HTTPS traffic, which subverts the purpose of SSL Manager and creates a lot of unnecessary overhead.

Why do some HTTPS sites not load properly?

HTTPS pages can fail to load, or only partially load, for a variety of reasons.

Here is a set of frequently accessed HTTP and HTTPS sites that often cause problems with Web proxy servers, including Content Gateway. Affected sites include:

- Microsoft Update
- Skype
- WebEx
- Real Networks Real Player
- Citrix collaboration products
- Firefox Update
- Yahoo! Messenger with Pidgin messaging client
- Logitech Messenger Agent and VirtualBox

Here are 2 Websense Technical Library articles that discuss these problem sites:

- Dropped HTTPS connections
- Web sites that have difficulty transiting Content Gateway

What causes ‘Peer sudden disconnect’ errors?

See Verify Deny: Peer Suddenly Disconnected Found.

What do my users need to know about HTTPS certificate verification?

Explain to them that:

- HTTPS is designed to provide secure connections and transmission of data.
- HTTPS sites, connections, and transmission of data are vulnerable to attack and compromise.
- A key element of HTTPS security is the exchange of signed digital certificates.
- When an HTTPS connection is being established, certificate verification is performed to validate the authenticity of the responding Web site, and to protect you and your network.
- Sometimes certificate verification checks fail, usually for valid reasons.
- Sometimes certificate verification checks fail in error, or for obscure reasons that your administrator will have to investigate.
- In most cases, certificate verification failure will block you from accessing the site.
- If your connection request fails due to a certificate verification failure, look carefully at the URL you are requesting to ensure that it does not have any typos.

- Ask a colleague if she or he is experiencing the same problem. If other colleagues are not, see if you can determine why not (what's different). If other colleagues are, report the problem to your Helpdesk.

How do I copy a certificate from my browser to the CA tree?

1. From the certificate window in your browser, select and open the desired certificate. Then, select the **Details** tab.
2. Select **Copy to File** to open the Certificate Export Wizard, then select **Next**.
3. Select **Base-64 encoded x.509 (.CER)**. Then, select **Next**.
4. Choose a file name and location to save the certificate. Then, select **Next**.
5. Select **Finish**.
6. Import the certificate from the location that it was saved to in step 4 to the CA tree by going to **Configure > SSL > Certificates > Add Root CA**.

How do I check and update a CRL link?

1. Go to the CA Tree (**Configure > SSL > Certificates > Certificate Authorities**).
2. Select the site to view or update the CRL link. To update the CRL link, click **Edit**.
3. Click **Submit** to save your changes.

Known Issues

A list of known issues is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the link above takes you to a login prompt. Log in to view the list.

Additional Resources

- HTTP Secure (Wikipedia)
- Transport Layer Security (Wikipedia)
- Digital certificate authority (IBM Software Information Center)
- Digital Certificates (Microsoft)
- The First few Milliseconds of an HTTPS Connection

Below is a sample of online SSL certificate checking tools. For more, use an Internet Search tool and search for "SSL checker".

- http://www.sslshopper.com/ssl-checker.html
- http://www.digicert.com/help/
- http://www.geocerts.com/ssl_checker

Glossary

Certificate Revocation List (CRL)

The Certificate Revocation List is used to check a certificate's revocation state and includes a list of certificates that have been issued and subsequently revoked by a given Certification Authority (CA).

Certificate Verification Engine (CVE)

The Certificate Verification Engine verifies certificates and checks for revoked certificates within the Websense SSL Manager.

Common Name (CN)

A Common Name is composed of the host + domain name that is used to identify the location being accessed.

Explicit proxy

An explicit proxy is configured within the application and is visible to the client. The client is explicitly configured to use a proxy server in which the browser knows that all requests will go through the proxy. Unlike Transparent proxy, each desktop must be configured to run explicit proxy.

Online Certificate Status Protocol (OCSP)

The Online Certificate Status Protocol is used to check a certificate’s revocation state and can be used separately or as a backup in conjunction with CRL. This allows the end host to query the OCSP server about a certificate’s revocation state at the time the certificate is presented.

Secure Sockets Layer (SSL)

Secure Sockets Layer is the standard security technology for establishing an encrypted link between a Web server and a browser. This link ensures that all data passed between the Web server and browser remains private and protected.

Server Name Indication (SNI)

The Server Name Indication (SNI) indicates what hostname the client is attempting to connect to at the start of the handshaking process. SNI allows multiple secure sites to be served off of the same IP address without requiring those sites to use the same certificate.

Subject Alternative Name (SAN)

Subject Alternative Names protect multiple hostnames with a single certificate after specifying a list of hostnames to be protected.

Transparent proxy

A transparent proxy is not configured within the application and is not visible to the client. The client does not know the traffic is being processed by a proxy other than the origin server. Unlike Explicit proxy, a transparent proxy typically intercepts all of the traffic for all IP addresses on a specified port.

Transport Layer Security (TLS)

Transport Layer Security (TLS), predecessor to Secure Sockets Layer (SSL), is the protocol that provides secure HTTP (HTTPS) for Internet transactions between Web browsers and Web servers.

Uniform Resource Identifier (URI)

A Uniform Resource Identifier (URI) identifies points of content such as a page of text, a video, a sound clip, a still or animated image, or a program.

Uniform Resource Locator (URL)

Uniform Resource Locator is the unique address for a Web site or file that is accessible on the Internet.

Web Cache Communication Protocol (WCCP)

Web Cache Communication Protocol (WCCP) transparently redirects users to cache servers without having to configure proxy settings in their browsers.