

# Application: Evaluating security vulnerabilities for SSL certificates

1. **Overview page:** Includes a summary of security issues.

**Security rating**

Overall rating	Certificate status	Certificate and chain attributes	Optimal server setup	Known security risks
<b>Not Secure</b>				

**Increase your certificate security rating!**  
Review and resolve these security issues. The certificate security rating will be updated after the next scan.

**⊘ To fix your Not secure rating:**

Multiple wildcard characters in one common name is not widely supported in client applications. Make sure the common name includes only one wildcard character, followed by a dot, then followed by a valid domain name (\*.example.com) or subdomain name (\*.subdomain.example.com).

Make sure that the server hosting this certificate supports TLS/SSL cipher suites that support symmetric encryption key sizes of 256 bits or greater. If the server does not support this, update the web server or load balancer software.

For each certificate in the chain, make sure that a valid CRL URL is found in the certificate's CRL Distribution Point (CDP) extension. Also make sure a valid OCSP URL is found in the Authority Information Access (AIA) extension.

**⚠ To avoid problems in the future:**

Make sure that all intermediate CA certificates in the chain use the SHA-256 hash algorithm. After 2016-Dec-31, modern browsers will

**Close**

2. **Certificate status page:** No problems found.

**Security rating**

Overall rating	Certificate status	Certificate and chain attributes	Optimal server setup	Known security risks
<b>Not Secure</b>				

Certificate status rating: **Secure**

Criteria	Result
Is the certificate validity date current?	Yes
Is the certificate valid (not expired or revoked)?	Yes
▶ Can the certificate revocation status be verified?	Verified

**Close**

3. Certificate chain page: Includes a warning for SHA-1 certificates.

The screenshot shows a 'Security rating' window with a navigation bar at the top. The 'Overall rating' is 'Not Secure'. The 'Certificate and chain attributes' section is highlighted and shows a rating of 'At Risk'. Below this is a table with the following data:

Criteria	Result
Root CA key strength	RSA2048
Intermediate CA key strength	Very Secure
End entity key strength	RSA2048
Root CA hash algorithm strength	SHA1
Intermediate CA hash algorithm strength	At Risk
GlobalSign Organization Validation CA - G2	SHA1
Make sure that all intermediate CA certificates in the chain use the SHA-256 hash algorithm. After 2016-Dec-31, modern browsers will not trust certificates that use SHA-1.	
End entity hash algorithm strength	SHA1
Use an SSL certificate with the SHA-256 hash algorithm. After 2016-Dec-31, modern browsers will not trust certificates that use SHA-1.	
Is this an Extended Validation (EV) certificate?	No, Organization Validation

A 'Close' button is located at the bottom right of the window.