
AVI
Networks®
Client SSL
Certificate
Validation
Avi Technical Reference (v17.2)
Copyright © 2018

Client SSL Certificate Validation

view online

Overview

Avi Vantage can validate SSL certificates presented by clients against a trusted certificate authority (CA) and a configured certificate revocation list (CRL). Certificate information is passed to the server through various HTTP headers through additional options. For certificate authentication, an HTTP application profile and an associated PKI profile have to be configured. This article explains HTTP profile and PKI profile configurations.

HTTP Profile

To configure an HTTP application profile, navigate to Templates > Profiles > HTTP Profile > Security. To know more, refer to Configuring HTTP Profile

Validation Type

The Client SSL Certificate Validation section displays three options for validation as discussed below.

- None: On selecting None as the Validation Type, client certificates will not be validated. If the virtual service is terminating SSL/TLS connections, the client's certificate will be ignored.
- Request: On selecting Request as the Validation Type, the clients should present a client certificate. If the client does not present a certificate, or if the certificate fails the CRL check, the client connection and requests are still forwarded to the destination server in an HTTP header. This enables the server to determine if the client can be allowed.
- Required: On selecting Required as the Validation Type, the client should present a valid certificate. The certificate must pass the CRL check defined in the PKI profile. The client certificate, or relevant fields, may still be passed to the server through HTTP headers.

PKI Profile

The public key infrastructure (PKI) profile contains the configured certificate authorities and the CRL. A PKI profile is not necessary if the Validation Type is set to Request, but is required if it is set to Require.

HTTP Headers

Avi Vantage optionally inserts the client's certificate, or parts of it, into a new HTTP header to be sent to the server. To insert multiple headers, the plus icon is used. These inserted headers are in addition to any headers added or manipulated by the more granular HTTP policies or DataScripts.

- HTTP Header Name: Name of the headers to be inserted into the client request that is sent to the server.
- HTTP Header Value: Used with the HTTP Header Name field, this field is used to determine the field of the client certificate to insert into the HTTP header sent to the server. Several options are more general, such as the SSL Cipher, which lists the ciphers negotiated between the client and Avi Vantage. These generic headers may be used for non-client certificate connections by setting the Validation Type to Request. ### PKI Profile

The PKI profile supports configuring and updating the client certificate revocation lists. The PKI profile is used to validate clients or server certificates.

Refer to Create a PKI Profile to know more.

- Client Certificate Validation: Avi Vantage validates client access to an HTTPS virtual service via client SSL certificates. Clients will present their certificate when accessing the virtual service. This will be matched against a CRL. If the certificate is valid and the clients are not on the list of revoked certificates, they will be allowed access to the HTTPS virtual server. Client certificate validation is enabled via the HTTP profile?s Authentication tab. The HTTP profile will reference the PKI profile for specifics on the CA and the CRL. A single PKI profile may be referenced by multiple HTTP profiles.

- Server Certificate Validation: Avi Vantage can validate the certificate presented by a server, such as when an HTTPS health check is sent to a server. Server certificate validation also uses a PKI profile to validate the certificate presented. Server certificate validation can be configured by enabling SSL within the desired pool, then specifying the PKI Profile.

PKI Profile Settings

- Name: The unique name for the profile.
- Ignore Peer Chain: If Ignore Peer Chain is enabled, the certificate validation will ignore any intermediate certificates that might be presented. The presented certificate is only checked against the final root certificate for revocation. This option is disabled by default. When disabled, the certificate must present a full chain which is traversed and validated, starting from the client or server presented certificate to the terminal root certificate. Each intermediate certificate must be validated and matched against a CA certificate included in the PKI profile.
- Host Header Check: If enabled, this option ensures the virtual service's VIP field, when resolved using DNS, matches the domain name field of the certificate presented from a server to Avi Vantage when back-end SSL is enabled. If the server's certificate does not match, it is considered insecure and marked down.
- Enable CRL Check: If Enable CRL Check is enabled, the client's certificate will be verified against the certificate revocation list.

For more information, refer to Create a PKI Profile

Certificate Authority

Add a new certificate from a trusted Certificate Authority. If more than one CA are included in the PKI profile, then a client's certificate should match one of them to be valid. A client's certificate must match the CA as the root of the chain. If the presented certificate has an intermediate chain, then each link in the chain must be included here. Enable Ignore Peer Chain to ignore intermediate validation checking.

Certificate Revocation List

The CRL allows invalidation of certificates (serial number). The revocation list may be updated by manually uploading a new CRL, or by periodically downloading from a CRL server. If a client or server certificate is found to be in the CRL, the SSL handshake will fail, with a resulting log created to provide further information about the handshake.

- Leaf Certificate CRL validation only: When enabled, Avi Vantage will only validate the leaf certificate against the CRL. The leaf is the next certificate in the chain up from the client certificate. A chain may consist of multiple certificates. To validate all certificates against the CRL, disable this option. Disabling this option means you need to upload all the CRLs issued by each certificate in the chain. Even if one CRL is missing, the validation process will fail.
- Server URL: Specify a server from which CRL updates can be downloaded. Access to this server will be done from the Avi Controller IP addresses, which means they will require firewall access to this destination. The CRL server may be identified by an IP address or a fully qualified domain name (FQDN) along with an HTTP path, such as https://www.avinetworks.com/crl.
- Refresh Time: After the elapsed period of time, Avi Vantage will automatically download an updated version of the CRL. If no time is specified, Avi Vantage will download a new CRL at the current CRL's lifetime expiration.
- Upload Certificate Revocation List File: Navigate to a CRL file for upload. Subsequent CRL updates can be done by manually uploading newer lists, or configuring the Server URL and Refresh Time to automate the process.