

Client Certificates & OCSP

Renard Schöpfel

DACH Region Technical Kemping

25.Sep.2026



Agenda

- Updates to Technical Kemping & Channel
- Client Certificates
- OCSP
- Questionnaire – Your Options matter

Kommende Termine

❖ Technical Kemping

❖ Die nächsten Termine:

❖ 23.Jan.2026

~~How to limit access to my applications & LM Backups~~

❖ 20.Mar.2026

~~Waf Essentials Unlocked~~

❖ 22.May.2026

~~IDS & Content rules for Body Modification~~

❖ 25.Sep.2026

~~Client Certificates & OCSP~~

❖ 20.Nov.2026

❖ Andere Webinare/Themen

❖ LoadMaster Trainings auf Deutsch

<https://www.infinigate.com/de/akademie/hersteller-spezifische-trainings/progress-trainings/>

❖ Progress|Kemp Masterclass

<https://events.teams.microsoft.com/event/99760272-2961-4975-b902-800c34cccbfb@db266a67-cbe0-4d26-ae1a-d0581fe03535>

Vergangene Kempings in DACH

- 01.09.2023 ESP OIDC & LDAP Loadbalancing <https://www.youtube.com/watch?v=XL6ZW1wmnrE>
- 17.11.2023 - ESP Advanced SAML & Integration of LoadMaster into Monitoring Solutions <https://www.youtube.com/watch?v=yOR4SoC4X1s>
- 26.01.2024 - ACME Certificate Automatization & Kemp Security Best Practices <https://www.youtube.com/watch?v=WkYTG2eniN8>
- 15.03.2024 - Virtual Service - The Magic of Sub Virtual Services & ESP - Authentictaion Options <https://www.youtube.com/watch?v=-10afouK5O0>
- 17.05.2024 - IDS/IPS & WAF - How to write Content Match Rules that generate Logs when triggered <https://www.youtube.com/watch?v=ghICS3W95bc>
- 20.09.2024 - WAF Fine Tuning & Healthchecks https://www.youtube.com/watch?v=9ypblUKo_bs
- 22.11.2024 - Adaptive balancing & Access Control Options https://www.youtube.com/watch?v=ZdvEdb_RGws
- 14.Feb.2025 - Technical Kemping: Virtual Service Backups und Zero Trust Concept <https://www.youtube.com/watch?v=Q1VTYF2KG14>
- 28. März 2025 - Reverse Proxy & API deep dive <https://www.youtube.com/watch?v=dqKs06e8Wrc>
- 16. Mai. 2025 - ESP - MFA Options, LoadMaster WAF and PCI DSS <https://www.youtube.com/watch?v=zrgMUuFCJfQ>
- 19. Sep. 2025 - LM Landingpage & LM Routing <https://www.youtube.com/watch?v=C4wZb5C7pgs>
- 14.Nov. 2025 - LM ESP OIDC&SAML & LM Logs <https://www.youtube.com/watch?v=LDGgCeqxYIU>
- 23. Jan. 2026 - How to limit access to my applications & LM Backups <https://www.youtube.com/watch?v=QBKqV8OlggE>
- 20. Mar. 2026 - Waf Essentials Unlocked <https://www.youtube.com/watch?v=gbuTmGLWFAo>
- 20.May.2026 - IDS & Content rules for Body Modification <https://www.youtube.com/watch?v=7JlwQlqvM6E>



Rénard Schöpfel

Principal Pre-Sales Engineer EMEA@ Progress

Email/Teams: renard.schoepfel@progress.com

Office: +49 221 65089777

- With Kemp since 2016

Previous Stations in Life:

- Dell
- Apple
- Kemp Support

LoadMaster EMEA Pre-Sales Team



Michael O'Brien

Michael.O'Brien@progress.com

Primary Regions:

UK, Ireland, Nordics, Eastern,
Southern, Africa, META



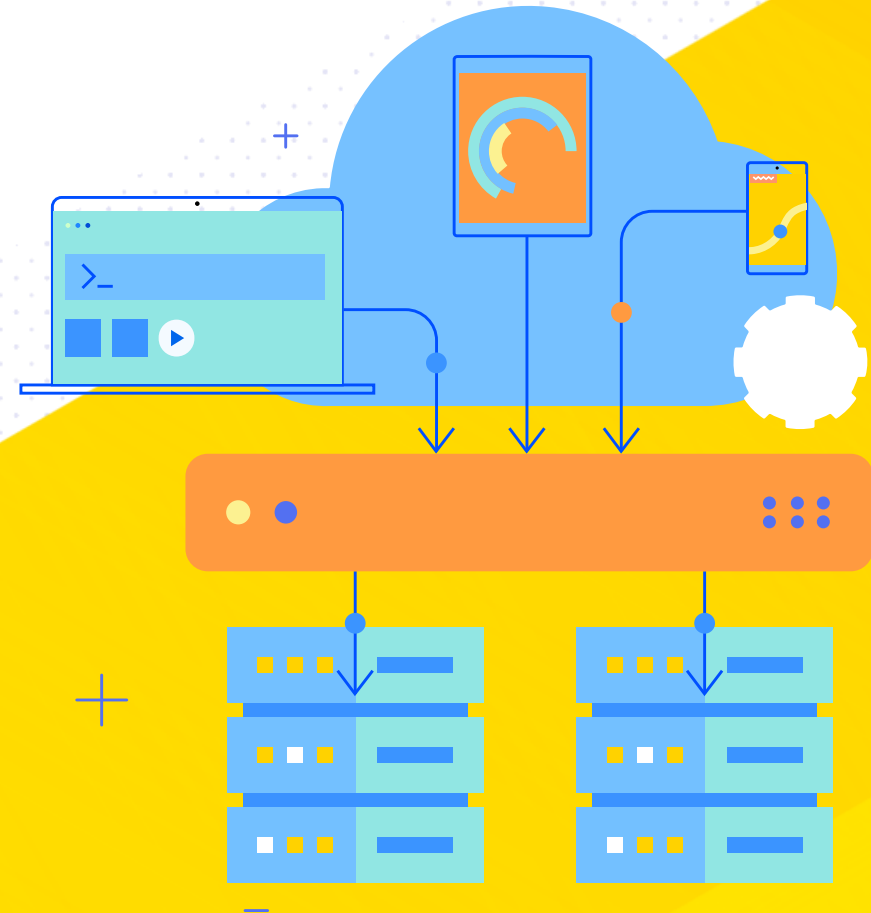
Renard Schöpfel

Renard.Schoepfel@progress.com

Primary Regions:

DACH & Benelux & France

Client Certificates



Why client certificates?

- Passwords prove that a user knows a secret
- Client certificates prove possession of the corresponding private key
- The private key remains on the client and is not sent across the network
- Client certificates can identify:
 - users
 - managed workstations
 - services
 - API clients
 - smart cards
- Useful where access must be limited before the application receives any traffic
- Particularly useful for privileged portals, partner access, machine-to-machine communication and administrative interfaces

TLS versus mutual TLS

- Normal TLS:
 - server presents a certificate
 - client validates the server
- Mutual TLS:
 - server presents a certificate
 - client also presents a certificate
 - both sides establish identity
- On an SSL-accelerated LoadMaster Virtual Service, the client TLS session terminates at the LoadMaster
- LoadMaster can require the client certificate under **SSL Properties > Client Certificates**

What does LoadMaster validate?

- A client certificate is presented during the TLS handshake.
- The certificate must be signed by a trusted CA.
- The relevant root and intermediate CA certificates must be available to LoadMaster.
- The certificate must be within its validity period.
- The certificate must contain the expected purpose and identity information.
- If OCSP checking is used, LoadMaster also requests the certificate's revocation status.
- A successful TLS handshake proves possession of the private key corresponding to the certificate.

Client certificates without ESP

- SSL Acceleration enabled on the Virtual Service.
- Client certificate set to required.
- LoadMaster acts as the mTLS enforcement point.
- A client without a certificate cannot complete the TLS connection.
- A client with an untrusted or invalid certificate is rejected.
- The backend application can remain unaware of the client certificate.
- Best suited for:
 - device-based admission control
 - protected administration portals
 - API or service access
 - simple certificate-gated web applications

Client certificates with ESP

- ESP adds application-layer pre-authentication.
- **Client Authentication Mode: Client Certificate**
- ESP can use certificate identity data as part of user authentication
- Supported ESP server-side choices depend on the firmware and configuration.
- Client-certificate authentication with **Server Authentication Mode: None** is supported from firmware 7.2.53.
- This permits certificate pre-authentication while the Real Server continues to use its own login mechanism.
- Client-certificate authentication is configured at the top-level Virtual Service because the TLS exchange happens there. Different SubVS client-side authentication modes cannot bypass that top-level certificate requirement.

Why expiry checking is not enough

Bullet points:

- Expiration is planned end-of-life.
- Revocation is unplanned early termination.
- Typical revocation reasons:
 - private key suspected of compromise
 - lost device or smart card
 - user or system no longer authorized
 - certificate issued incorrectly
 - certificate replaced
- Revocation needs a status source:
 - Certificate Revocation List, or CRL
 - Online Certificate Status Protocol, or OCSP

How OCSP works

- The certificate may contain an OCSP responder URL in its **Authority Information Access**, or AIA, extension.
- LoadMaster sends the certificate status request to the responder.
- The relevant responses for explaining the concept are:
 - good
 - revoked
 - unknown
- The responder signs its response.
- The relying party uses the response when deciding whether to trust the certificate.
- An OCSP response is not a replacement for chain or date validation. It supplements them.

For LoadMaster, the OCSP service configured globally is described as a fallback when the certificate does not specify an OCSP server in its AIA information. If both are present, the certificate's AIA information takes precedence.

Failure policy and operational risk

This can trigger a useful customer discussion:

- What should happen when the certificate is valid but the OCSP responder cannot be reached?
- **Fail closed** (deny access; stronger security; OCSP availability becomes part of application availability)
- **Fail open** (continue accepting the client certificate; higher availability; revoked certificates may temporarily be accepted)
- LoadMaster exposes **Allow Access on Server Failure**, which treats a connection failure or timeout as though the OCSP response were valid.
- This is an explicit risk decision, not merely a technical convenience.
- The OCSP responder, DNS, routing and firewall rules become security dependencies.
- For a production design, monitoring the responder is essential.

OCSP checking versus OCSP stapling

Client-certificate OCSP checking

- LoadMaster validates the revocation state of a certificate presented by a client.

OCSP stapling

- LoadMaster serves cached OCSP information about its **Virtual Service certificate** to clients that request it.
- This helps clients validate the LoadMaster's server certificate.
- It is not the same as validating an incoming client certificate.

The LoadMaster OCSP documentation calls out OCSP checking and OCSP stapling separately and says that stapling returns cached status information for Virtual Service certificates.

Useful Links

- <https://docs.progress.com/bundle/loadmaster-configuration-guide-web-user-interface-wui-ga/page/OCSP-Configuration.html>
- <https://docs.progress.com/bundle/loadmaster-technical-note-loadmaster-hardening-ga/page/Configure-OCSP.html>
- <https://learn.microsoft.com/windows-server/identity/ad-cs/>

Life Demo

Demo 1: Ordinary HTTPS

Demo 2: Require a client-certificate

Optional 3: ESP

Demo 4: Revoke the certificate



- 2026-09-23T08:56:40+02:00 vlma1 ocspd: Invalid HTTP response code 500
- 2026-09-23T08:56:40+02:00 vlma1 vsslproxy: OCSP verify failed (/DC=com/DC=progressdemo/CN=Users/CN=Administrator/emailAddress=Administrator@progressdemo.com)
- 2026-09-23T09:34:08+02:00 vlma1 vsslproxy: OCSP verify failed (/DC=com/DC=progressdemo/CN=Users/CN=Administrator/emailAddress=Administrator@progressdemo.com)
- 2026-09-23T09:36:45+02:00 vlma1 occheck: Cfg LDAP_SERVER : Valid ()
- 2026-09-23T09:36:45+02:00 vlma1 occheck: Cfg LDAP_BACKSERVER :

ocsp

No.	Time	Source	Destination	Protocol	Length	Info
4	2026-09-23 09:34:08.046614	192.168.100.10	192.168.100.20	OCSP	271	Request
5	2026-09-23 09:34:08.047762	192.168.100.20	192.168.100.10	OCSP	270	Response

> Frame 5: Packet, 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits)

> Ethernet II, Src: VMware_8a:ad:b8 (00:50:56:8a:ad:b8), Dst: VMware_9a:25:a7 (00:50:56:9a:25:a7)

> Internet Protocol Version 4, Src: 192.168.100.20, Dst: 192.168.100.10

> Transmission Control Protocol, Src Port: 80, Dst Port: 49914, Seq: 1, Ack: 218, Len: 216

> Hypertext Transfer Protocol

Online Certificate Status Protocol

responseStatus: unauthorized (6)

0000 00 50 56 9a 25 a7 00 50 56 8a ad b8 08 00 45 00 ·PV·%·P V·····E·

0010 01 00 f2 43 40 00 80 06 be 44 c0 a8 64 14 c0 a8 ···C@·····D···d··

0020 64 0a 00 50 c2 fa f7 9f a1 cf d2 38 a9 64 50 19 d··P·······8·dP·

0030 20 02 87 bc 00 00 48 54 54 50 2f 31 2e 31 20 32 ·····HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 43 6f 6e 00 OK··C ache-Con

0050 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a trol: no -cache··

0060 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Content- Type: ap

0070 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 73 70 2d 72 plicatio n/ocsp-r

0080 65 73 70 6f 6e 73 65 0d 0a 53 65 72 76 65 72 3a esponse ·Server:

0090 20 4d 69 63 72 6f 73 6f 66 74 2d 49 49 53 2f 31 Microso ft-IIS/1

00a0 30 2e 30 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 0.0·X-P owered-B

00b0 79 3a 20 41 53 50 2e 4e 45 54 0d 0a 44 61 74 65 y: ASP.N ET··Date

00c0 3a 20 57 65 64 2c 20 32 33 20 53 65 70 20 32 30 : Wed, 2 3 Sep 20

00d0 32 36 20 30 37 3a 33 34 3a 30 38 20 47 4d 54 0d 26 07:34 :08 GMT·

00e0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f ·Connect ion: clo

00f0 73 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 se··Cont ent-Leng

0100 74 68 3a 20 35 0d 0a 0d 0a 30 03 0a 01 06 th: 5··· ·0···.

Progress®

© 2026 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

21

