

**UOC Sistemi Informativi**

Direttore ing. Giorgio Roncolato

Prot. n. 147129

Verona, 20/08/2025

Alla c.a Responsabili
Istituti/privati accreditati;
Residenze Sanitarie Assistenziali;
Onlus o associazioni di volontariato;
Fornitori di servizi per AULSS 9 Scaligera

OGGETTO: attivazione “Autenticazione a Più Fattori” (MFA) - 15 settembre 2025.

Gent.mi sig.ri,

Richiamati la L. n. 90/2024, “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”, il D.lgs. n. 138/2024 che recepisce la direttiva (UE) 2022/2555 relativa a misure per aumentare il livello di “cybersicurezza”, nonché il rapporto intitolato “[La minaccia cibernetica al settore sanitario](#)”, pubblicato dall’Agenzia per la Cybersicurezza Nazionale (ACN) nel portale <https://www.acn.gov.it/portale/csirt-italia>, e vista l’informativa del servizio “Cybersecurity Threat Intelligence” del CERT di Regione del Veneto che segnala possibili attacchi informatici alle aziende sanitarie, è necessario ed urgente adottare misure di mitigazione del rischio.

Pertanto, a partire dal **15 settembre 2025** le politiche di sicurezza dell’Azienda ULSS n. 9 prevederanno **obbligatoriamente** metodi di autenticazione a più fattori (MFA) per l’accesso a tutti i sistemi informatici utilizzabili attraverso Internet oppure tramite accesso da remoto.

Cosa Cambia?

Per le connessioni da remoto ai sistemi informatici interni, via VPN SSL con FortiClient, e per l’accesso a sistemi informatici Web dell’Azienda ULSS n. 9 Scaligera esposti in internet, verrà attivata la pre-autenticazione con credenziali di dominio AULSS9 (username e password) ed un terzo codice di sicurezza variabile (OTP - One Time Password) inviato, ad ogni accesso, sullo smartphone personale o tramite messaggio e-mail nella casella di posta elettronica individuale.

Nell’apposita sezione del portale Internet aziendale <https://www.aulss9.veneto.it/applicativi> sono disponibili i manuali:

- “[Manuale per l’accesso a risorse Web di AULSS9 con autenticazione MFA](#)“ per l’accesso ai sistemi applicativi Web esposti in internet;
- “[Accesso a risorse informatiche di AULSS9 con autenticazione MFA via VPN SSL Forticlient](#)“ per l’accesso a server ed applicazioni tramite VPN SSL.



Cosa accade se non ci si adegua?

Il mancato adeguamento alle nuove politiche di sicurezza dell'azienda ULSS n. 9 comporta la revoca all'accesso ai servizi interni disponibili tramite VPN con FortiClient e a tutti i sistemi applicativi Web esposti in Internet, (p.es. protocollo-scaligera.aulss9.veneto.it, cus.aulss9.veneto.it, portale-scaligera.aulss9.veneto.it, woe.aulss9.veneto.it, ecc.)

Cosa devo fare?

Le aziende private con un contratto attivo e gli enti/istituti in possesso di una convenzione in corso di validità devono inviare l'elenco aggiornato di tutti gli operatori in servizio già dotati di credenziali applicative dell'AULSS9, integrando con il numero di telefono cellulare e la mail personale tramite apposito modulo allegato.

Per gli operatori attualmente privi delle credenziali **applicative** e per tutte le nuove richieste future, la procedura rimane invariata e si dovrà contattare il competente ufficio dell'azienda ULSS n. 9 Scaligera.

Ho dei dubbi, chi contatto?

Ai destinatari di questa comunicazione si ricordano le attività da espletare:

- inviare via mail a gestionedto@aulss9.veneto.it **entro il 6 settembre 2025** il modulo allegato [ICTS C01C-2.3-Modulo.Richiesta.Credenziali.e.Accesso.da.Remoto](#);
- consultare i manuali di accesso pubblicati nel portale AULSS9.

Eventuali richieste di assistenza vanno indirizzate alla casella e-mail: assistenzamfa@aulss9.veneto.it oppure chiamare il numero telefonico 045 8075555.

Ringraziando anticipatamente per la collaborazione, si porgono distinti saluti.

Il Direttore
UOC Sistemi Informativi
Ing. Giorgio Roncolato

UOC Sistemi Informativi
Responsabile del procedimento ing. Giorgio Roncolato
Referente dell'istruttoria: r.p. Alessandro Fascina
e-mail: amministrazione.sistemi.informativi@aulss9.veneto.it