

Suite di crittografia supportate da Umbrella

Sommario

[Introduzione](#)

[Panoramica](#)

[Suite di crittografia approvate da PSB](#)

Introduzione

Questo documento descrive le suite di cifratura supportate da Umbrella.

Panoramica

Cisco Umbrella accetta le suite di cifratura menzionate quando negozia le connessioni HTTPS a, e a monte da, Secure Web Gateway (SWG), Intelligent Proxy e le pagine bloccate. Per connettersi correttamente a tali servizi, i client devono supportare almeno una delle suite di cifratura indicate.

La base di riferimento per la sicurezza dei prodotti (PSB) di Cisco definisce i requisiti di sicurezza per la funzionalità, lo sviluppo e il test. Una parte di questi requisiti guida l'elenco delle suite di cifratura supportate. Questi sono documentati qui per scopi informativi e non sono configurabili in Umbrella.

Suite di crittografia approvate da PSB

ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES256-GCM-SHA384	TLS_AES_256_GCM_SHA384
AES128-GCM-SHA256	TLS_AES_128_GCM_SHA256

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).