Aggiorna gli endpoint al supporto di TLS 1.2 per Umbrella Services

Sommario

- Introduzione
- Panoramica dei requisiti di TLS 1.2
- Aggiornamenti al supporto di TLS 1.0/1.1
- Protezione per dispositivi AnyConnect o client mobili
- Supporto Secure Web Gateway
- Requisiti di Umbrella Active Directory Connector
- Agenti Umbrella: Requisiti minimi di versione
  - Windows Roaming Client o modulo AnyConnect
  - macOS Roaming Client o AnyConnect Module
- Domande frequenti aggiuntive
  - Cosa succede se gli endpoint non vengono aggiornati entro la scadenza?
  - La chiave del Registro di sistema funziona per le versioni precedenti?
  - È possibile testare solo TLS 1.2?
  - Perché deprecare TLS 1.0 e 1.1?
  - Perché è stato scelto il 31 marzo 2020?
  - Questo può avere un impatto sugli utenti con dispositivi aggiornati?
  - Dopo l'aggiornamento di un endpoint per TLS 1.2, sono necessarie ulteriori azioni per riattivare il supporto Umbrella?
  - Come si conferma il supporto dell'endpoint per TLS 1.2?
    - Supporto browser Web Windows
    - Supporto di Windows .NET Framework
    - Per Mac e altri sistemi

Introduzione

Questo documento descrive come preparare endpoint e applicazioni per i servizi Umbrella che richiedono TLS 1.2.

Panoramica dei requisiti di TLS 1.2

Al 31 marzo 2020, Transport Layer Security (TLS) 1.0 e 1.1 non sono più supportati dai server e dai servizi Umbrella. Per funzionare correttamente con Umbrella, tutti gli endpoint devono supportare TLS 1.2.

Aggiornamenti al supporto di TLS 1.0/1.1

- Ad eccezione di AnyConnect, Umbrella Roaming Client e AD Connector, Umbrella ha

terminato il supporto per TLS 1.0/1.1 a marzo 2020.
- A causa delle dipendenze backend, alcuni servizi dashboard e API hanno continuato ad accettare connessioni TLS 1.0/1.1 fino al 27 gennaio 2021. Dopo questa data, questi servizi non accettano più le connessioni TLS 1.0/1.1.
- I dispositivi che non possono accedere al dashboard o alle API devono essere controllati per verificare il supporto di TLS 1.2.

Protezione per dispositivi AnyConnect o client mobili

Umbrella ha esteso la scadenza al 27 gennaio 2021 per completare l'aggiornamento a TLS 1.2. Non esistono ulteriori estensioni. I dispositivi AnyConnect e Roaming Client che non soddisfano i requisiti TLS 1.2 dopo il 27 gennaio 2021 non ricevono più la protezione da Umbrella.

Supporto Secure Web Gateway

- Umbrella non supporta il traffico HTTPS che utilizza TLS 1.0 o 1.1 nel prodotto Secure Gateway.
- Prima del 27 gennaio 2021, Secure Web Gateway offriva supporto limitato per questi protocolli solo quando la decrittografia HTTPS era disabilitata.
- Configurare tutti i sistemi operativi client per il supporto di TLS 1.2.
- Aggiornare o modificare le applicazioni non browser in base alle esigenze per garantire la compatibilità con TLS 1.2. Contattare i fornitori delle applicazioni per assistenza.

Requisiti di Umbrella Active Directory Connector

Umbrella non supporta i connettori di Active Directory distribuiti nei sistemi operativi Windows che hanno raggiunto la fine del ciclo di vita. I connettori AD in esecuzione su versioni di Windows non supportate (Windows Server 2008, 2008 R2 o Windows 7) interrompono la sincronizzazione con Umbrella e immettono lo stato di errore il 27 gennaio 2021.

Agenti Umbrella: Requisiti minimi di versione

Windows Roaming Client o modulo AnyConnect

- Client roaming Cisco Umbrella: Versione 2.2.356 o successiva
- Cisco AnyConnect con modulo di roaming Umbrella: Versione 4.8.02042 o successiva
- Per utilizzare una versione client precedente, configurare TLS 1.2 tramite le modifiche del Registro di sistema di Windows (vedere i passaggi seguenti).
- Microsoft .NET Framework: Versione 4.6.2 o successiva oppure Windows 7 con patch con .NET 3.5.1
  (AnyConnect richiede .NET 4.x o versione successiva)
- Versioni di Windows supportate: 7, 8, 8,1, 10

macOS Roaming Client o AnyConnect Module

- Qualsiasi versione di Umbrella Roaming Client o del modulo di roaming AnyConnect supporta TLS 1.2
- Versione macOS supportata: 10.9 o successiva

Domande frequenti aggiuntive

Cosa succede se gli endpoint non vengono aggiornati entro la scadenza?

Gli endpoint che non sono in grado di negoziare una connessione TLS 1.2 non possono accedere ai sistemi Umbrella, inclusi il dashboard, i servizi proxy intelligenti e le pagine di blocco.
Per i clienti che eseguono il modulo Umbrella Roaming in AnyConnect, il client Umbrella Enterprise Roaming o il connettore Umbrella AD, il client non può connettersi ad alcun servizio Umbrella. Di conseguenza, il client non sincronizza la configurazione e lo stato con il dashboard Umbrella.

I client in roaming esistenti interrompono l'attivazione e rimangono non protetti al successivo avvio del servizio. I nuovi client che non supportano TLS 1.2 non possono eseguire la registrazione con Umbrella. Questi client non funzionano; Il DNS continua a risolversi tramite lo stack di rete locale, ma i servizi di sicurezza dei client mobili non vengono attivati.

I dispositivi che tentano di accedere ai siti bloccati o quelli instradati tramite il proxy intelligente non possono connettersi. I dispositivi che utilizzano il client di roaming non possono accedere ai siti Web Umbrella, bloccare le pagine o i servizi proxy.

La chiave del Registro di sistema funziona per le versioni precedenti?

Sì, per AnyConnect. Continuare a utilizzare le versioni precedenti dopo aver applicato la modifica del Registro di sistema per preferire la crittografia avanzata. Prima delle versioni minime elencate, il client mobile ha avviato le connessioni HTTPS senza specificare TLS 1.2 strongcrypto in modo esplicito. Se .NET supporta TLS 1.2, viene utilizzato per impostazione predefinita. Le chiavi del Registro di sistema impongono a .NET di utilizzare l'algoritmo di crittografia, replicando gli aggiornamenti nelle nuove versioni del client. I client mobili autonomi precedenti all'ultima versione non sono supportati.

È possibile testare solo TLS 1.2?

Sì. Disabilitare TLS 1.0 e TLS 1.1 nel Registro di sistema di Windows per verificare che i dispositivi funzionino correttamente utilizzando solo TLS 1.2.

Perché deprecare TLS 1.0 e 1.1?

TLS 1.0 e 1.1 sono obsoleti e non supportano i moderni algoritmi di crittografia. Contengono vulnerabilità che gli aggressori possono sfruttare. L'Internet Engineering Task Force ha deprecato entrambi i protocolli. La maggior parte del traffico Internet crittografato utilizza TLS 1.2, che è stato introdotto più di dieci anni fa.

Perché è stato scelto il 31 marzo 2020?

In questo arco di tempo, il settore sta deprecando TLS 1.0 e 1.1. Google, Microsoft, Apple, e Mozilla hanno annunciato che i loro browser non supportano più TLS 1.0 e 1.1 a partire da marzo 2020.

Questo può avere un impatto sugli utenti con dispositivi aggiornati?

No. La maggior parte dei siti Web supporta TLS 1.2. Secondo Qualys SSL Labs, il 95,2% dei siti Web supporta TLS 1.2. Questo numero dovrebbe aumentare con l'avvicinarsi di marzo 2020. Un numero limitato di siti Web non può funzionare, ma l'impatto complessivo sugli utenti è minimo. Assicurarsi che i dispositivi aggiornati includano la versione corretta di .NET per i computer Windows.

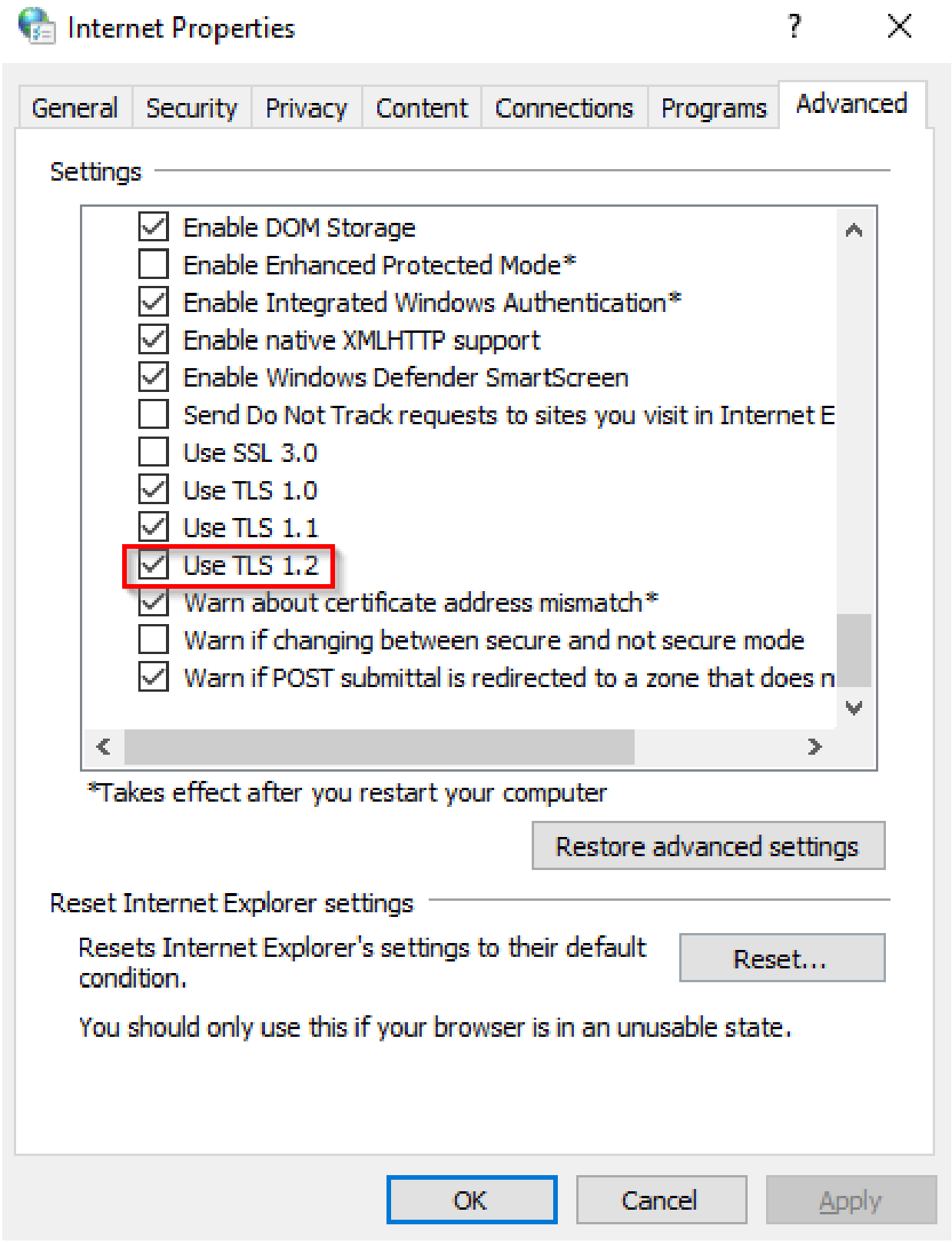
Dopo l'aggiornamento di un endpoint per TLS 1.2, sono necessarie ulteriori azioni per riattivare il supporto Umbrella?

Nella maggior parte dei casi non sono necessarie ulteriori azioni. Il client ristabilisce la comunicazione con i sistemi Umbrella utilizzando il protocollo sicuro TLS 1.2. Per il client Umbrella Enterprise Roaming o per AnyConnect, il ripristino può richiedere un ritardo se il sistema è stato offline durante un aggiornamento software del client. Il client deve scaricare gli aggiornamenti prima del ripristino completo del servizio.

Come si conferma il supporto dell'endpoint per TLS 1.2?

- Supporto browser Web Windows
    - Accedi al dashboard Umbrella e ai siti Web correlati.
    - Eseguire il test del browser dei laboratori SSL. Confermare che accanto a TLS 1.2 nella sezione Protocolli venga visualizzato il messaggio "Sì".

- Supporto di Windows .NET Framework
    - Si applica a Enterprise Roaming Client, AnyConnect Roaming Module o AD Connector.
    - .NET 4.6.2 o versione successiva fornisce il supporto TLS 1.2 nativo.
    - Le versioni precedenti richiedono modifiche del Registro di sistema (4.x) o del Registro di sistema e patch di hotfix manuali (3.5).
    - Queste informazioni si applicano al software Umbrella in esecuzione su .NET Framework, inclusi AD Connector e Roaming Client.
    - Disabilitare SSL, TLS 1.0 e TLS 1.1 a livello di sistema operativo completando le istruzioni fornite da Microsoft.



blobid0.png

- Per Mac e altri sistemi
- Eseguire il [test del browser SSL Labs](). Confermare che accanto a TLS 1.2 nella sezione

Protocolli venga visualizzato il messaggio "Sì".

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).