# Häufige Fehler bei Zertifikaten und TLS-Protokollen

## Inhalt



## Einleitung

In diesem Dokument werden häufige Fehler in Zertifikaten und TLS-Protokollen bei der Umbrella Dashboard Activity Search beschrieben.

## Überblick

Der aufgrund von Zertifikat- und TLS-Fehlern blockierte HTTP-Datenverkehr kann jetzt auf der Umbrella Dashboard Activity Search angezeigt werden. Dieser Artikel enthält eine Liste gängiger Fehlermeldungen sowie eine kurze Erläuterung der einzelnen Fehler.

## Zertifikatfehler

### Upstream-Zertifikat abgelaufen

Ein von der Website vorgelegtes Zertifikat ist abgelaufen. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

### Upstream-Zertifikat selbstsigniert

Das von der Website präsentierte Serverzertifikat ist nicht von einer Zertifizierungsstelle signiert, sodass Umbrella nicht feststellen kann, ob das Zertifikat vertrauenswürdig ist.

Selbst signierte Zertifikate werden manchmal verwendet, wenn ein Server eine Ressource hostet, die für eine eingeschränkte Zielgruppe bestimmt ist. So verwenden Webportale für IT-Sicherheitsanwendungen häufig standardmäßig selbstsignierte Zertifikate. Umbrella kann nicht so konfiguriert werden, dass selbstsignierte Zertifikate als vertrauenswürdig angesehen werden.

## Zwischenzertifikat fehlt

Umbrella war nicht in der Lage, Zertifikate für alle zwischengeschalteten Stellen zu erhalten und konnte daher nicht die gesamte Vertrauenskette validieren.

Webserverzertifikate werden in der Regel von einem Zwischenzertifikat einer Zertifizierungsstelle ausgestellt/signiert. Diese Zwischenzertifikate können auch durch andere Zwischenzertifikate ausgestellt werden. Das Webserverzertifikat (auch als "Endblattzertifikat" bezeichnet) und alle Zwischenzertifikate bilden eine Kette zurück zu einem Stammzertifikat. Die Website muss die Zwischenzertifikate mit dem Serverzertifikat bündeln, damit Umbrella die gesamte Vertrauenskette validieren kann. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

Wenn das Zertifikat die Erweiterung "Authority Information Access" (Zugriff auf Autoritätsdaten) enthält, versucht Umbrella, die zwischengeschalteten CAs automatisch abzurufen. Beachten Sie, dass Umbrella die AIA-Erweiterung nur unterstützt, wenn HTTPS-Entschlüsselung und Dateiinspektion aktiviert sind.

## Fehlender Antragstellername für das Upstream-Zertifikat.

Das Feld "Betreff" des Zertifikats enthält keinen DN (Distinguished Name) zur Identifizierung des Zertifikats. Dies ist eine Anforderung für alle Zertifikate, die von einer Zertifizierungsstelle ausgestellt wurden und daher von Cisco Umbrella verlangt werden. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

## Für das Upstream-Zertifikat fehlt ein allgemeiner Name.

Das von der Website vorgelegte Zertifikat hat keinen gemeinsamen Namen. Das Feld "Common Name (CN)" wird von Umbrella SWG benötigt. Dieser enthält den Zertifikathostnamen, der erforderlich ist, um zu überprüfen, ob das Zertifikat mit der vom Benutzer angeforderten Ressource (z. B. Die im Browser eingegebene Adresse). Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

## Upstream-Zertifikat nicht vertrauenswürdig

Das Zertifikat ist von Cisco Umbrella nicht vertrauenswürdig. Dieser Fehler bedeutet in der Regel, dass Cisco der Stammzertifizierungsstelle, die das Zertifikat ausgestellt hat, nicht vertraut.

Umbrella SWG verfügt über eine integrierte Liste von bekannten vertrauenswürdigen Stammzertifizierungsstellen, die wir von einer seriösen Quelle aktualisieren. Wenn das Zertifikat

der Website nicht von einer Zertifizierungsstelle in dieser Liste signiert wird, schlägt die Zertifikatvalidierung fehl. Wenn Sie glauben, dass Umbrella eine vertrauenswürdige Stammzertifizierungsstelle fehlt, wenden Sie sich an den technischen Support.

### Der Hostname in Zertifikat unterscheidet sich von dem erwarteten.

Die vom Benutzer angeforderte Ressource (z. B. die im Browser eingegebene Adresse) stimmt nicht mit dem Common Name (CN) oder Subject Alternative Name (SAN) des Zertifikats überein. Umbrella kann dem Zertifikat für diese Anforderung daher nicht vertrauen. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

### Upstream-Zertifikat widerrufen

Das von der Website bereitgestellte Zertifikat wurde von der ausstellenden Zertifizierungsstelle widerrufen.

Umbrella führt OCSP-Prüfungen (Online Certificate Status Protocol) durch, um festzustellen, ob ein Zertifikat später von einer Zertifizierungsstelle widerrufen wurde. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

## TLS-Handshake-Fehler

### Nicht unterstützte Upstream-Verschlüsselung

Der TLS-Handshake konnte nicht abgeschlossen werden. Dies bedeutet in der Regel, dass die Website keine der Cipher Suites unterstützt, die von Umbrella SWG verwendet werden. Dieser Fehler kann bei älteren oder veralteten Webservern auftreten, die nur schwächere TLS-Chiffren unterstützen. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

### Upstream-TLS-Versionskonflikt

Der TLS-Handshake konnte nicht abgeschlossen werden, da die Website nicht dieselbe TLS-Version unterstützt, die Umbrella SWG verwendet. Derzeit unterstützt Umbrella SWG Proxy TLS 1.2 und TLS 1.3 sowohl auf den Client-seitigen Verbindungen zu Umbrella SWG als auch von Umbrella SWG Proxy-Verbindungen zu Ziel-Webservern.

### Upstream-DH-Schlüssel kleiner als 1024 Bit

Der TLS-Handshake konnte nicht abgeschlossen werden, da die Website einen schwachen Diffie-Hellman-Schlüssel verwendet, der von Umbrella nicht unterstützt wird. Wenden Sie sich an den Webmaster der Website, um dieses Problem zu melden.

## Problemumgehungen

Sie können diese Probleme umgehen, indem Sie Konfigurationsänderungen in Cisco Umbrella vornehmen. Dies muss nur geschehen, wenn Sie der Authentizität des Servers und des Zertifikats

vertrauen.

Workarounds können mit einem Eintrag in der "Selektiven Entschlüsselungsliste" angewendet werden, um die Entschlüsselung zu deaktivieren, oder mit einem Eintrag in der Liste "Externe Domänen", um den Datenverkehr von Umbrella vollständig zu umgehen. Umbrella führt keine Zertifikatsüberprüfung durch, wenn die Entschlüsselung deaktiviert ist. Beachten Sie, dass der Browser in den meisten Fällen immer noch einen Fehler oder eine Warnung anzeigt, wenn der Datenverkehr von Umbrella umgangen wird - Webbrowser führen eine ähnliche Zertifikatsvalidierung durch.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.