



Zertifikatsfehler im Browser - Zugriff verweigern

Ein Leser hatte mich gestern angeschrieben, mit der Bitte im zu zeigen, wo die Einstellungen im Gruppenrichtlinieneditor zu finden sind.

Es geht darum, den Benutzern keine Möglichkeit einzuräumen, sofern der jeweilige Browser ein Problem mit einem Zertifikat erkannt hat, diesen Fehlerhinweis zu umgehen, und die Webseite trotz Hinweis auf eine Gefahr zu besuchen.

Dafür bieten die Hersteller in ihren ADMX-Vorlagen entsprechende Einstellmöglichkeiten an.

Die Browser überprüfen mit verschiedenen Mechanismen, ob der Name der aufgerufenen (geschützten) Webseite (SSL/TLS) auch im Zertifikat an den entsprechenden Stellen Subject, SAN vorkommt. Wird keine Übereinstimmung gefunden sollte der Browser die Verbindung ablehnen, um vor einer möglichen Gefahr zu schützen.

Das machen aber nicht alle Browser aus dem Karton heraus! Um den Schutz zu aktivieren benötigt wir zuerst alle ADMX Dateien für die jeweiligen Browser.

<https://www.gruppenrichtlinien.org/downloads/>

Die Einstellungen für den Internet Explorer finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer/Internetsystemsteuerung

Editor für lokale Gruppenrichtlinien

Datei Aktion Ansicht ?

Internet Explorer > Internetsystemsteuerung

Ignorieren von Zertifikatsfehlern verhindern

Richtlinieneinstellung bearbeiten

Anforderungen:
Mindestens Internet Explorer 7.0

Beschreibung:
Diese Richtlinieneinstellung verhindert, dass der Benutzer SSL/TLS-Zertifikatsfehler (Secure Socket Layer/Transport Layer Security), die die Navigation in Internet Explorer unterbrechen (z. B. "Abgelaufen", "Gesperrt" oder "Name stimmt nicht überein") ignoriert.

Wenn Sie diese Richtlinieneinstellung aktivieren, kann der Benutzer das Browsen nicht mehr fortsetzen.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, kann der Benutzer entscheiden, ob Zertifikatsfehler ignoriert werden sollen und das Browsen fortsetzen.

Einstellung	Status	Kommentar
Inhaltsseite	Nicht konfiguriert	Nein
Seite "Allgemein"	Nicht konfiguriert	Nein
Seite "Erweitert"	Nicht konfiguriert	Nein
Sicherheitsseite	Nicht konfiguriert	Nein
Seite "Erweitert" deaktivieren	Nicht konfiguriert	Nein
Verbindungsseite deaktivieren	Nicht konfiguriert	Nein
Inhaltsseite deaktivieren	Nicht konfiguriert	Nein
Seite "Allgemein" deaktivieren	Nicht konfiguriert	Nein
Datenschutzseite deaktivieren	Nicht konfiguriert	Nein
Programmseite deaktivieren	Nicht konfiguriert	Nein
Sicherheitsseite deaktivieren	Nicht konfiguriert	Nein
Internationale Domännennamen senden	Nicht konfiguriert	Nein
UTF-8 für mailto-Links verwenden	Nicht konfiguriert	Nein
Ignorieren von Zertifikatsfehlern verhindern	Aktiviert	Nein

10 Einstellung(en)

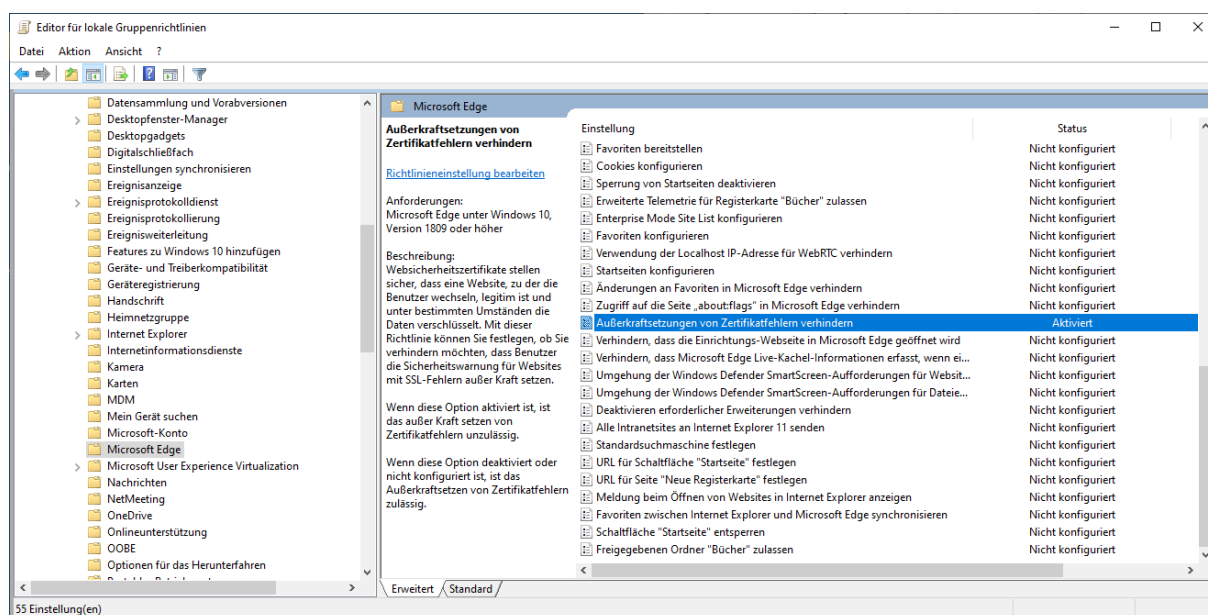
Erweitert / Standard



Zertifikatsfehler im Browser - Zugriff verweigern

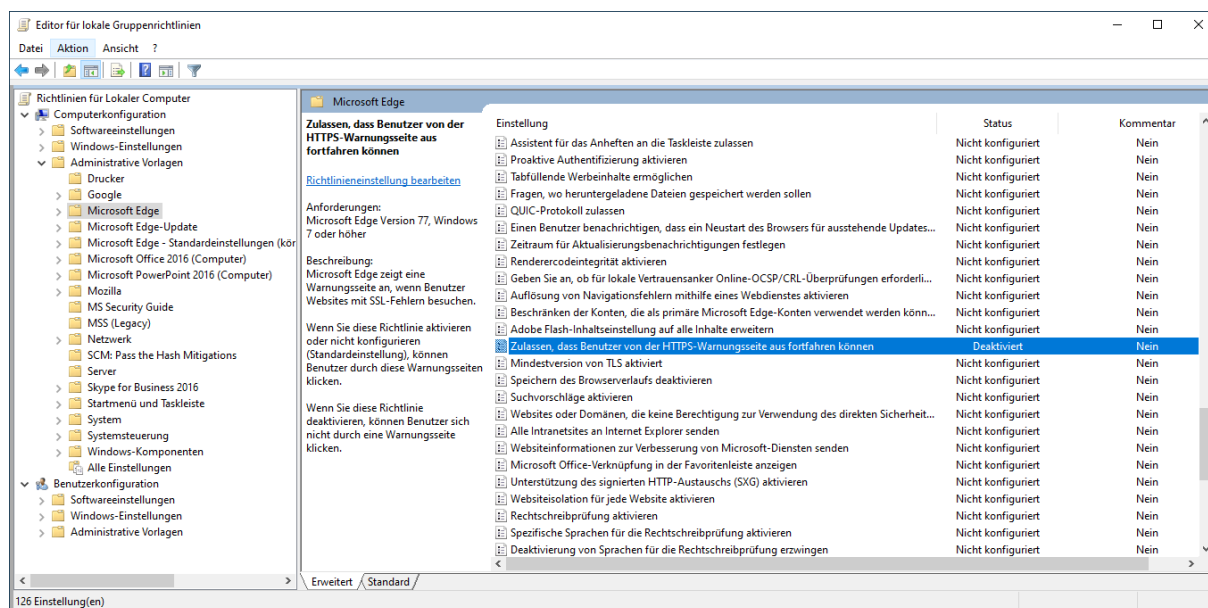
Die Einstellungen für den Microsoft Edge finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Microsoft Edge



Die Einstellungen für den Microsoft Edge-Chromium Browser finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Microsoft Edge





Zertifikatsfehler im Browser - Zugriff verweigern

Die Einstellungen für den Google Chrome finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Google/Google Chrome

The screenshot shows the 'Editor für lokale Gruppenrichtlinien' (Local Group Policy Editor) window. The left pane shows the tree structure: 'Computerkonfiguration' > 'Administrative Vorlagen' > 'Google' > 'Google Chrome'. The right pane displays the 'Fortfahren von SSL-Hinweiseite erlauben' (Continue on SSL warning page) policy. The policy is currently 'Deaktiviert' (Disabled). The description states: 'Chrome zeigt eine Seite mit einer Warnmeldung an, wenn Nutzer Websites aufrufen, die SSL-Fehler aufweisen. Standardmäßig oder bei Festlegung von "true" für diese Richtlinie ist es Nutzern gestattet, durch diese Seiten mit Warnmeldung zu klicken. Wenn für die Richtlinie "false" festgelegt wird, können Nutzer nicht mehr durch diese Seiten klicken.' The list of settings on the right includes: 'Enable Ambient Authentication for profile types' (Nicht konfiguriert), 'Enable stricter treatment for mixed content' (Nicht konfiguriert), 'Erforderliche Registrierung für Cloud Management aktivieren' (Nicht konfiguriert), 'Erlaubt einer Seite, während des Unloads Pop-ups einzublenden' (Nicht konfiguriert), 'Ermöglicht verwalteten Erweiterungen, die Enterprise Hardware Platform API zu verwe...' (Nicht konfiguriert), 'Erstellung von Roaming-Kopien für Google Chrome-Profilaten aktivieren' (Nicht konfiguriert), 'Erzwingung der Zertifikatstransparenz für eine Liste alter Zertifizierungsstellen deaktivieren...' (Nicht konfiguriert), 'Erzwingung der Zertifikatstransparenz für eine Liste mit subjectPublicKeyInfo-Hashes ...' (Nicht konfiguriert), 'Erzwingung der Zertifikatstransparenz für eine Liste von URLs deaktivieren' (Nicht konfiguriert), 'Festlegen, wie Daten vom Chrome Cleanup Tool an Google gesendet werden' (Nicht konfiguriert), 'Festlegen, wo Entwicklertools verwendet werden können' (Nicht konfiguriert), 'Filterung von Inhalten nur für Erwachsene durch "SafeSites" konfigurieren.' (Nicht konfiguriert), 'Fortfahren von der Safe Browsing-Hinweiseite deaktivieren' (Nicht konfiguriert), 'Fortfahren von SSL-Hinweiseite erlauben' (Deaktiviert), 'Funktion "Zum Anrufen klicken" aktivieren' (Nicht konfiguriert), 'Gastmodus im Browser aktivieren' (Nicht konfiguriert), 'Gastmodus im Browser erzwingen' (Nicht konfiguriert), 'Gebietschema der App' (Nicht konfiguriert), 'Gespeicherte Passwörter bei erster Ausführung aus Standardbrowser importieren' (Nicht konfiguriert), 'Globales HTTP-Auth-Cache aktivieren' (Nicht konfiguriert), 'Google Cast erlauben, eine Verbindung zu Übertragungsgeräten unter allen IP-Adresse...' (Nicht konfiguriert), 'Google Chrome als Standardbrowser festlegen' (Nicht konfiguriert), 'Google SafeSearch erzwingen' (Nicht konfiguriert), 'Hardwarebeschleunigung verwenden, falls verfügbar' (Nicht konfiguriert), 'Inkognitomodus - Verfügbarkeit' (Nicht konfiguriert), 'Integriertes DNS Client verwenden' (Nicht konfiguriert).

Die Einstellungen für den Mozilla Firefox finden wir hier:

Computerkonfiguration/Administrative Vorlagen/Mozilla/Firefox

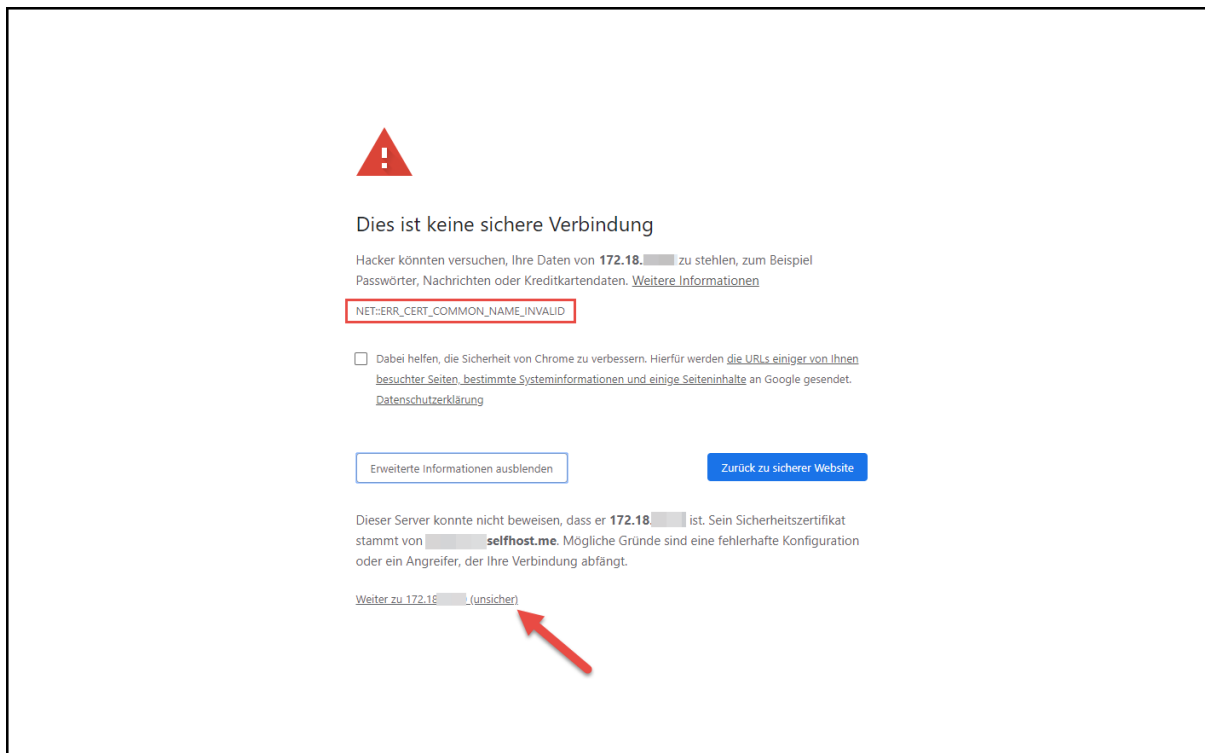
The screenshot shows the 'Editor für lokale Gruppenrichtlinien' (Local Group Policy Editor) window. The left pane shows the tree structure: 'Computerkonfiguration' > 'Administrative Vorlagen' > 'Mozilla' > 'Firefox'. The right pane displays the 'Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten' (Prevent adding exceptions for insecure certificates) policy. The policy is currently 'Aktiviert' (Enabled). The description states: 'Wenn Sie die Richtlinieneinstellung aktivieren, steht "Ausnahme hinzufügen" nicht zur Verfügung, wenn ein Zertifikat ungültig ist. Dies verhindert, dass ein Benutzer Zertifikatsfehler überschreibt. Wenn Sie die Richtlinieneinstellung deaktivieren oder nicht konfigurieren, steht "Ausnahme hinzufügen" zur Verfügung, wenn ein Zertifikat ungültig ist.' The list of settings on the right includes: 'Add-ons' (Nicht konfiguriert), 'Authentifizierung' (Nicht konfiguriert), 'Berechtigungen' (Nicht konfiguriert), 'Cookies' (Nicht konfiguriert), 'Einstellungen' (Nicht konfiguriert), 'Erweiterungen' (Nicht konfiguriert), 'Flash' (Nicht konfiguriert), 'Lesezeichen' (Nicht konfiguriert), 'Popups' (Nicht konfiguriert), 'Startseite' (Nicht konfiguriert), 'Suche' (Nicht konfiguriert), 'Zertifikate' (Nicht konfiguriert), 'Abfrage des Download Verzeichnisses' (Nicht konfiguriert), 'Abgesicherten Modus deaktivieren' (Nicht konfiguriert), 'Als Hintergrundbild einrichten deaktivieren' (Nicht konfiguriert), 'Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten' (Aktiviert), 'Ausnahmen zu gesperrten Webseiten' (Nicht konfiguriert), 'Benutzerdefinierte Update-URL' (Nicht konfiguriert), 'Betrugsversuch- und Schadprogrammschutz ändern' (Nicht konfiguriert), 'Captive Portal Unterstützung' (Nicht konfiguriert), 'Chronik deaktivieren' (Nicht konfiguriert), 'Die Chronik löschen, wenn Firefox geschlossen wird' (Nicht konfiguriert), 'DNS Over HTTPS konfigurieren' (Nicht konfiguriert), 'Download Verzeichnis' (Nicht konfiguriert), 'Feedback Commands deaktivieren' (Nicht konfiguriert), 'Firefox-Instanzen deaktivieren' (Nicht konfiguriert).



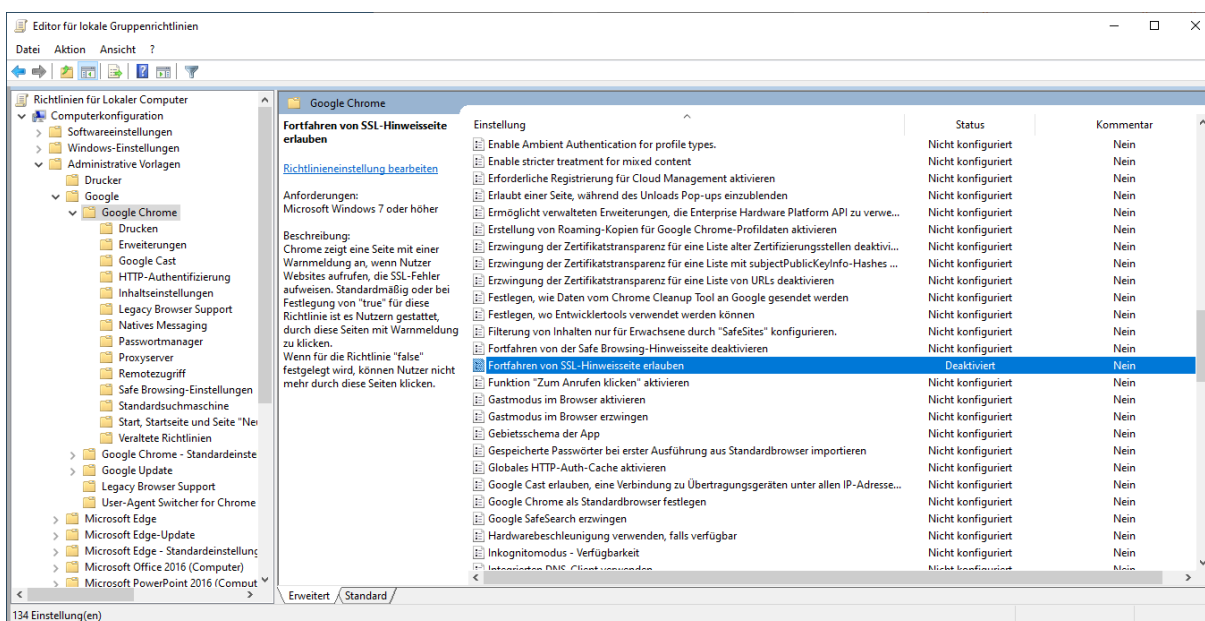
Zertifikatsfehler im Browser - Zugriff verweigern

Ein Beispiel in Aktion, wenn wir die Richtlinie für Google Chrome so einstellen, dass der Browser dahingehend gehärtet wird.

Ohne Härtung, bekommen wir die Möglichkeit geboten, den Hinweis mit Weiter zu 172.18.xx.xx (unsicher) zu umgehen, um die Webseite zu dennoch besuchen.



Schalten wir die Richtlinie „Ausnahme hinzufügen verhindern bei unsicheren Zertifikaten“ auf = Deaktiviert,





Zertifikatsfehler im Browser - Zugriff verweigern

...ist ein Umgehen des Hinweises nicht mehr möglich und die Webseite bleibt im Zugriff verhindert.



Dies ist keine sichere Verbindung

Hacker könnten versuchen, Ihre Daten von 172.18.1.1 zu stehlen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. [Weitere Informationen](#)

NET:ERR_CERT_COMMON_NAME_INVALID

☐ Dabei helfen, die Sicherheit von Chrome zu verbessern. Hierfür werden [die URLs einiger von Ihnen besuchter Seiten, bestimmte Systeminformationen und einige Seiteninhalte](#) an Google gesendet. [Datenschutzerklärung](#)

Erweiterte Informationen ausblenden

Neu laden

172.18.1.1 schützt Ihre Daten in der Regel durch Verschlüsselung. Als Google Chrome dieses Mal versuchte, eine Verbindung zu 172.18.1.1 herzustellen, gab die Website ungewöhnliche und falsche Anmeldedaten zurück. Entweder versucht ein Angreifer, sich als 172.18.1.1 auszugeben, oder die Verbindung wurde durch eine WLAN-Anmeldeseite unterbrochen. Da Google Chrome die Verbindung vor dem Austausch von Daten unterbrochen hat, sind Ihre Informationen weiterhin sicher.

Sie können 172.18.1.1 zurzeit nicht aufrufen, da die Website verschlüsselte Anmeldedaten gesendet hat, die von Google Chrome nicht verarbeitet werden können. Netzwerkfehler und Angriffe sind in der Regel nur vorübergehend, sodass die Seite wahrscheinlich später wieder funktioniert.