Verlängerung des Expressway-Zertifikats

Inhalt

Einleitung

In diesem Dokument wird die Verlängerung des Expressway/Video Communication Server (VCS)-Zertifikats beschrieben.

Die Informationen in diesem Dokument gelten für Expressway und VCS. Das Dokument verweist auf Expressway, dieser kann jedoch mit VCS ausgetauscht werden.

> **Anmerkung:** Dieses Dokument soll Sie bei der Erneuerung des Zertifikats unterstützen. Es empfiehlt sich jedoch, auch den Cisco Expressway Certificate Creation and Use Deployment Guide für Ihre Version zu lesen.

Hintergrundinformationen

Wenn ein Zertifikat erneuert werden soll, müssen zwei Hauptaspekte berücksichtigt werden, um sicherzustellen, dass das System auch nach der Installation des neuen Zertifikats ordnungsgemäß funktioniert:

1. Die Attribute des neuen Zertifikats müssen mit denen des alten Zertifikats übereinstimmen (hauptsächlich der alternative Antragstellername und die Verwendung des erweiterten Schlüssels).

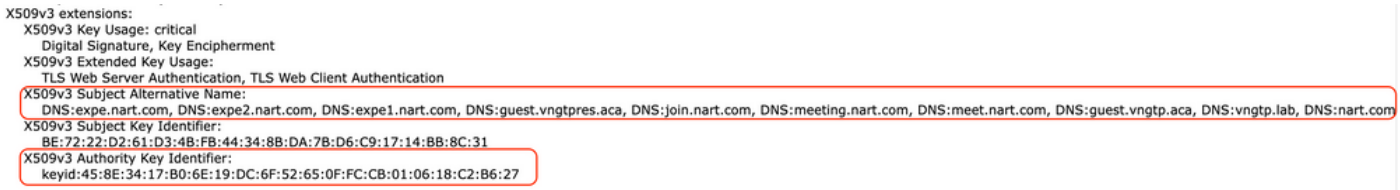
2. Die CA (Zertifizierungsstelle), die zum Signieren des neuen Zertifikats verwendet wird, muss von anderen Servern, die direkt mit dem Expressway kommunizieren, als vertrauenswürdig angesehen werden (z. B. CUCM, Expressway-C, Expressway-E usw.).

Prozess

A) Informationen aus dem aktuellen Zertifikat abrufen

1. Öffnen Sie Expressway Webpage **Maintenance > Security > Server certificate > Show decoded.**

2. Kopieren Sie in dem sich öffnenden neuen Fenster die X509v3-Erweiterungen "Subject Alternative Name" und "Authority Key Identifier" in ein Notebook-Dokument.

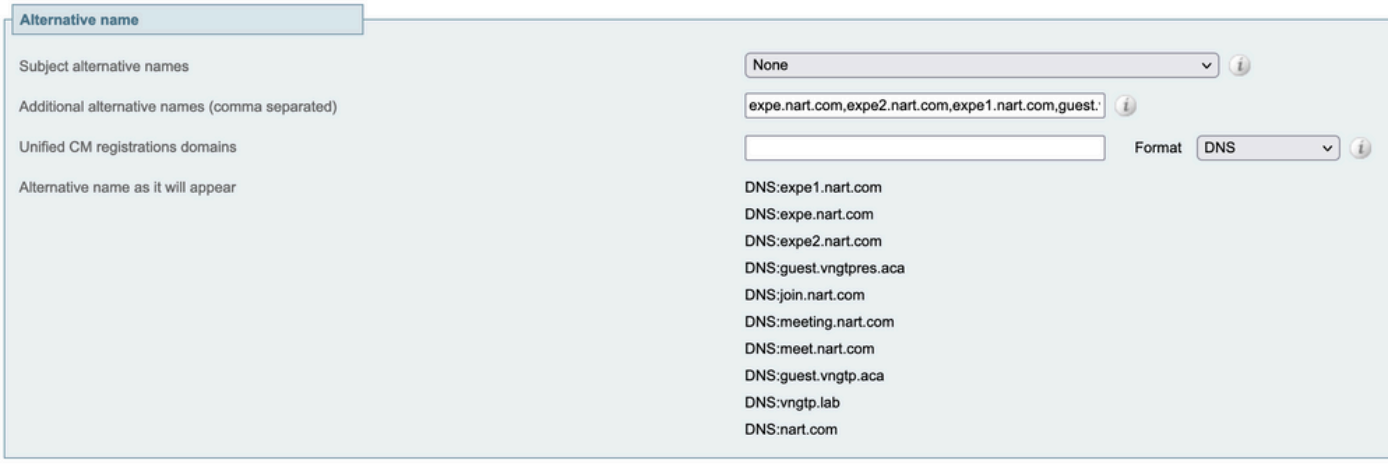


Fenster "Dekodiertes Zertifikat anzeigen"

B) Erstellen Sie die CSR-Anfrage (Certificate Signing Request), und senden Sie sie zur Signatur an die Zertifizierungsstelle (Certification Authority).

1. Aus Expressway Webpage **Maintenance > Security > Server certificate > Generate CSR.**

2. Geben Sie im Fenster CSR generieren im Feld **Zusätzliche alternative Namen (durch Komma getrennt)** alle Werte für "Subject Alternative Names" ein, die wir im Abschnitt A gespeichert haben, und entfernen Sie "DNS:" und trennen Sie die Liste durch Kommas, siehe Bild (Neben "Alternativer Name wie er angezeigt wird" finden Sie eine Liste aller SANs, die im Zertifikat verwendet werden sollen):



CSR SAN-Einträge generieren

3. Füllen Sie den Rest der Informationen unter dem Abschnitt **Zusätzliche Informationen** wie Land, Unternehmen, Bundesland usw. aus und klicken Sie auf **CSR erstellen.**

4. Nachdem Sie den CSR generiert haben, zeigt die Seite **Wartung > Sicherheit > Serverzertifikat** eine Option zum **Verwerfen von CSR** und **Herunterladen an.** Sie müssen **Herunterladen** auswählen und den CSR zur Signierung an die Zertifizierungsstelle senden.

> **Anmerkung:** Vergewissern Sie sich, dass Sie **CSR** nicht **verwerfen,** bevor das neue Zertifikat installiert ist. Wenn Sie **CSR verwerfen** und dann versuchen, ein mit dem CSR signiertes Zertifikat zu installieren, das verworfen wurde, schlägt die Zertifikatinstallation fehl.

C) Überprüfen Sie die SAN-Liste und das Attribut für die erweiterte/erweiterte Schlüsselverwendung im neuen Zertifikat.

Öffnen Sie das neu signierte Zertifikat im Windows-Zertifikats-Manager, und überprüfen Sie Folgendes:

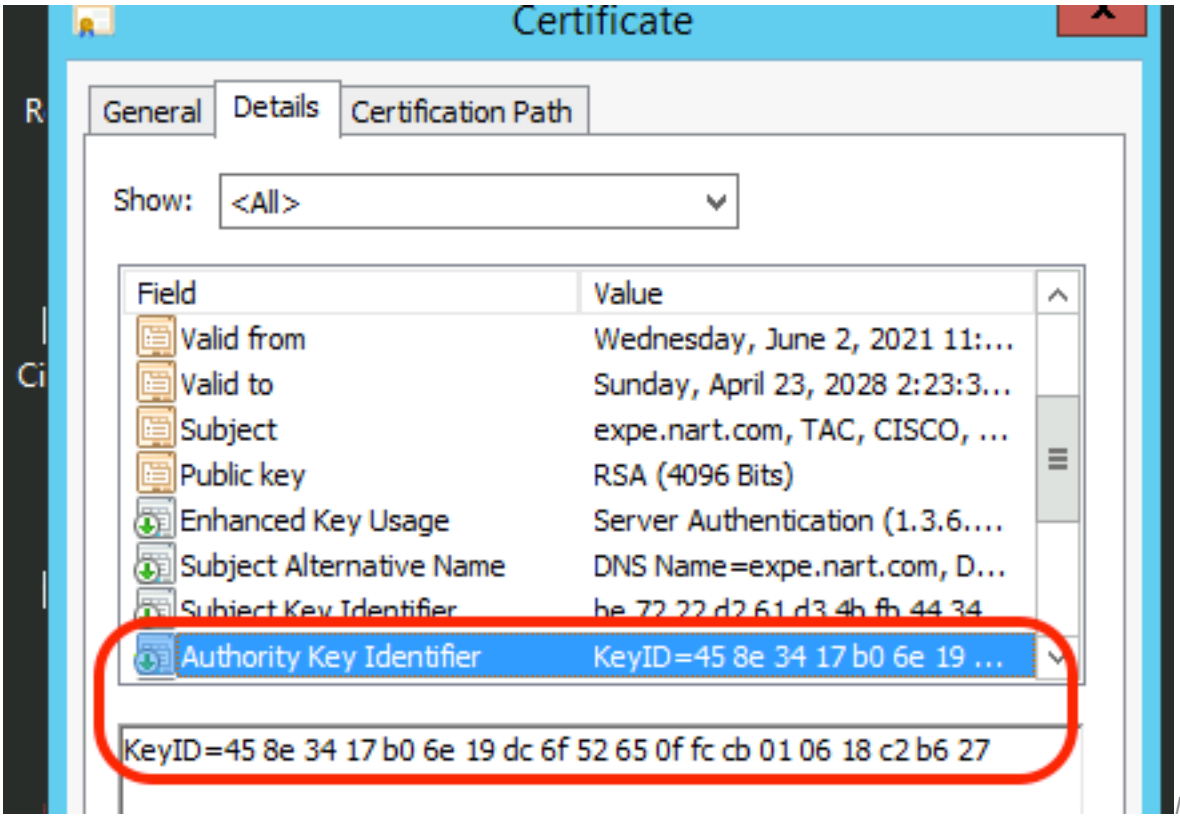
1. Die SAN-Liste stimmt mit der SAN-Liste überein, die wir im Abschnitt A gespeichert haben, in dem wir den CSR generiert haben.

2. Das Attribut "Extended/Enhanced key usage" muss sowohl "Client Authentication" als auch "Server Authentication" enthalten.

> **Anmerkung:** Wenn das Zertifikat die Erweiterung .pem aufweist, benennen Sie es in .cer oder .crt um, damit es mit dem Windows-Zertifikats-Manager geöffnet werden kann. Wenn das Zertifikat mit dem Windows-Zertifikats-Manager geöffnet wurde, können Sie zur Registerkarte **Details > In Datei kopieren** gehen und es als Base64-kodierte Datei exportieren. Eine Base64-kodierte Datei hat normalerweise "-----BEGIN CERTIFICATE-----" oben und "-----END CERTIFICATE-----" unten, wenn sie in einem Texteditor geöffnet wird.

D) Überprüfen Sie, ob die Zertifizierungsstelle, die das neue Zertifikat signiert hat, mit der Zertifizierungsstelle übereinstimmt, die das alte Zertifikat signiert hat.

Öffnen Sie das neu signierte Zertifikat im Windows-Zertifikatmanager, kopieren Sie den Wert "Authority Key Identifier", und vergleichen Sie ihn mit dem Wert "Authority Key Identifier", den wir in Abschnitt A gespeichert haben.



Neues Zertifikat wurde mit dem Windows-Zertifikats-Manager geöffnet

Wenn beide Werte identisch sind, bedeutet dies, dass das neue Zertifikat mit derselben Zertifizierungsstelle signiert wurde wie das alte Zertifikat. Sie können mit Abschnitt E fortfahren, um das neue Zertifikat hochzuladen.

Wenn sich die Werte unterscheiden, bedeutet dies, dass die zum Signieren des neuen Zertifikats verwendete Zertifizierungsstelle sich von der Zertifizierungsstelle unterscheidet, die zum Signieren

des alten Zertifikats verwendet wurde. Führen Sie hierzu die folgenden Schritte aus, bevor Sie mit Abschnitt E fortfahren können:

1. Rufen Sie alle Zertifikate der Zwischen-Zertifizierungsstelle (sofern vorhanden) und die Zertifikate der Stammzertifizierungsstelle ab.

2. Gehen Sie zu **Maintenance > Security > Trusted CA certificate** , klicken Sie auf **Browse**, suchen Sie dann nach dem Zwischenzertifikat auf Ihrem Computer und laden Sie es hoch. Führen Sie den gleichen Vorgang für alle anderen Zwischenzertifikate der Zertifizierungsstelle und das Stammzertifikat der Zertifizierungsstelle aus.

3. Führen Sie dasselbe auf jedem Expressway-E (wenn das zu erneuernde Zertifikat ein Expressway-C-Zertifikat ist) durch, der mit diesem Server verbunden ist, oder auf jedem Expressway-C (wenn das zu erneuernde Zertifikat ein Expressway-E-Zertifikat ist), der mit diesem Server verbunden ist.

4. Wenn es sich bei dem zu erneuernden Zertifikat um ein Expressway-C-Zertifikat handelt und Sie über MRA verfügen oder über sichere Zonen für CUCM verfügen, müssen Sie sicherstellen, dass CUCM der neuen Stamm- und Zwischen-CA vertraut und die Stamm- und Zwischen-CA-Zertifikate in CUCM-Tomcat-Trust- und Callmanager-Trust-Speicher hochladen und die relevanten Services auf CUCM neu starten.

E) Neues Zertifikat installieren

Nachdem Sie alle vorherigen Punkte überprüft haben, können Sie das neue Zertifikat jetzt auf dem Expressway installieren. Wählen Sie dazu **Wartung > Sicherheit > Serverzertifikat** auf **Durchsuchen** und wählen Sie die neue Zertifikatsdatei von Ihrem Computer aus und laden Sie sie hoch.

Sie müssen Expressway neu starten, nachdem Sie ein neues Zertifikat installiert haben.

> **Anmerkung:** Stellen Sie sicher, dass das Zertifikat, das Sie von **Maintenance > Security > Server Certificate** auf Expressway hochladen, nur das Expressway-Serverzertifikat und NICHT die vollständige Zertifikatskette enthält, und stellen Sie sicher, dass es ein Base64-Zertifikat enthält.

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.