CSM - Installieren von SSL-Zertifikaten von Drittanbietern für den GUI-Zugriff

Inhalt

Einführung

Cisco Security Manager (CSM) bietet eine Option zur Verwendung von Sicherheitszertifikaten, die von Zertifizierungsstellen (Certificate Authorities, CAs) von Drittanbietern ausgestellt wurden. Diese Zertifikate können verwendet werden, wenn die Organisationsrichtlinie die Verwendung von selbstsignierten CSM-Zertifikaten verhindert oder vorschreibt, dass Systeme ein von einer bestimmten Zertifizierungsstelle erworbenes Zertifikat verwenden müssen.

TLS/SSL verwendet diese Zertifikate für die Kommunikation zwischen dem CSM-Server und dem Clientbrowser. Dieses Dokument beschreibt die Schritte zum Generieren einer CSR-Anfrage (Certificate Signing Request) im CSM und zum Installieren der Identitäts- und Stammzertifikate der CA im selben Dokument.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der SSL-Zertifikatsarchitektur.
- Grundlegende Kenntnisse von Cisco Security Manager.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Security Manager Version 4.11 und höher

CSR-Erstellung über die Benutzeroberfläche

In diesem Abschnitt wird beschrieben, wie Sie eine CSR-Anfrage erstellen.

Schritt 1: Führen Sie die Cisco Security Manager-Startseite aus, und wählen Sie **Serververwaltung > Server > Sicherheit > Einzelserver-Management > Zertifikateinrichtung aus.**

Schritt 2: Geben Sie die erforderlichen Werte für die in dieser Tabelle beschriebenen Felder ein:

Feld	Nutzungsnotizen
Ländername	Ländercode aus zwei Zeichen
Bundesland	Zweistelliger Bundesland- oder Landesvorwahl oder vollständiger Name des Staate oder der Provinz.
Lokalität	Zwei Zeichen Stadt- oder Ortsvorwahl oder vollständiger Name der Stadt oder Stadt
Name der Organisation	Geben Sie den Namen Ihrer Organisation oder eine Abkürzung ein.
Name der Organisationseinheit	Geben Sie den Namen Ihrer Abteilung oder eine Abkürzung ein.
Servername	DNS-Name, IP-Adresse oder Hostname des Computers. Geben Sie den Servernamen mit einem geeigneten und auflösbare Domänennamen ein. Diese wird auf Ihrem Zertifikat angezeigt (ob selbstsigniert od von einem Dritten ausgestellt). Lokaler Host oder 127.0.0.1 sollte nicht angegebe werden.
E-Mail-Adresse	E-Mail-Adresse, an die die E-Mail gesendet werden muss.

Schritt 3: Klicken Sie auf **Apply**, um die CSR-Datei zu erstellen.

Der Prozess generiert die folgenden Dateien:

- server.key (Serverschlüssel): Der private Schlüssel des Servers.
- server.crt: Das selbstsignierte Zertifikat des Servers.
- server.pk8: Der private Schlüssel des Servers im PKCS#8-Format.
- server.csr - CSR-Datei (Certificate Signing Request).

Hinweis: Dies ist der Pfad für die generierten Dateien.
~CSCOpx\MDC\Apache\conf\ssl\chain.cer
~CSCOpx\MDC\Apache\conf\ssl\server.crt
~CSCOpx\MDC\Apache\conf\ssl\server.csr
~CSCOpx\MDC\Apache\conf\ssl\server.pk8
~CSCOpx\MDC\Apache\conf\ssl\server.key

Hinweis: Wenn es sich bei dem Zertifikat um ein selbstsigniertes Zertifikat handelt, können Sie diese Informationen nicht ändern.

Hochladen des Identitätszertifikats in den CSM-Server

In diesem Abschnitt wird beschrieben, wie das von der CA bereitgestellte Identitätszertifikat auf den CSM-Server hochgeladen wird.

Schritt 1 Suchen Sie das SSL Utility Script, das an dieser Stelle verfügbar ist

```
NMSROOT\MDC\Apache
```

Hinweis: NMSROOT muss durch das Verzeichnis ersetzt werden, in dem CSM installiert ist.

Dieses Dienstprogramm bietet diese Optionen.

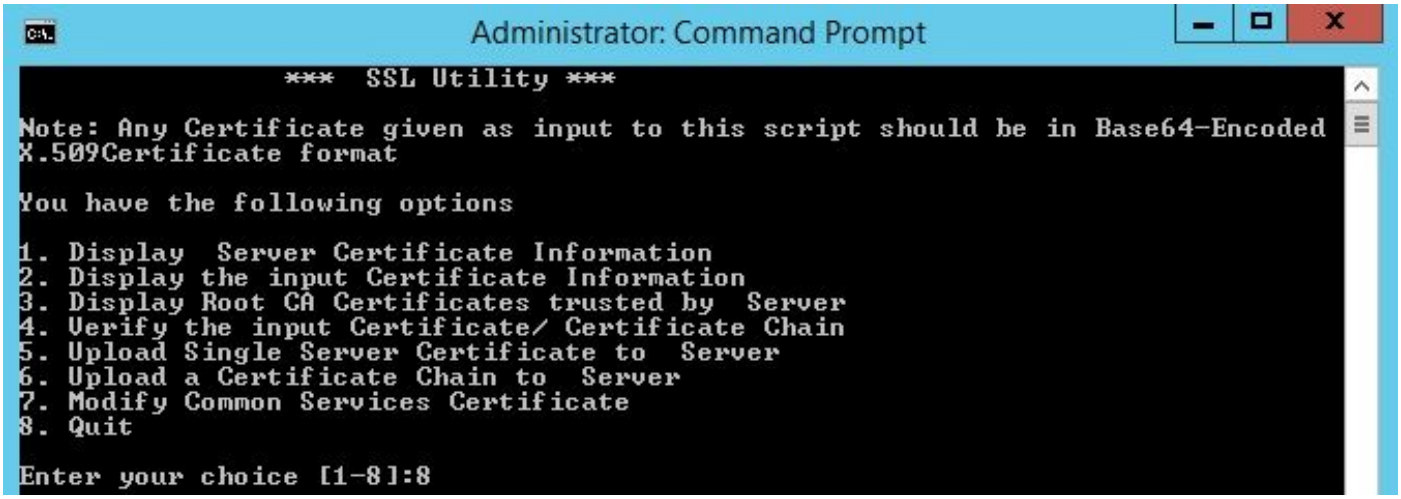
Nummer	Option	Vorteile
1	Serverzertifikatinformationen anzeigen	• Zeigt die Zertifikatdetails des CSM-Servers an. Bei von Dritten ausgestellten Zertifikaten werden mit dieser Option die Details des Serverzertifikats, ggf. die Zwischenzertifikate und das Zertifikat der Stammzertifizierungsstelle angezeigt.
2	Anzeigen der Informationen für das Eingabefeld	• Überprüft, ob das Zertifikat gültig ist. Diese Option akzeptiert ein Zertifikat als Eingabe und: • Überprüft, ob das Zertifikat im codierten X.509-Zertifikatsformat vorliegt. • Zeigt den Gegenstand des Zertifikats und die Einzelheiten des Zertifikats an. • Überprüft, ob das Zertifikat auf dem Server gültig ist.
1	Root-Zertifizierungsstellenzertifikate anzeigen, die vom Server	Erstellt eine Liste aller Zertifikate der Stammzertifizierungsstelle.

	vertrauenswürdig sind	Überprüft, ob das von CAs von Drittanbietern ausgestellte Serverzertifikat hochgeladen werden kann. Wenn Sie diese Option auswählen, wird das Dienstprogramm: • Überprüft, ob das Zertifikat im Base64-Format mit verschlüsseltem X.509Certificate vorliegt. • Überprüft, ob das Zertifikat auf dem Server gültig ist • Überprüft, ob der private Schlüssel des Servers und das Zertifikat des Eingabeservers übereinstimmen. • Überprüft, ob das Serverzertifikat auf das erforderliche Stammzertifizierungszertifikat zurückverfolgt werden kann, mit dem es signiert wurde. • Erstellt die Zertifikatskette, wenn auch die Zwischenketten angegeben werden, und überprüft, ob die Kette mit dem entsprechenden Zertifikat der Root-Zertifizierungsstelle endet.
4	Überprüfen Sie das Eingangszertifikat oder die Zertifikatkette.	Nachdem die Überprüfung erfolgreich abgeschlossen wurde, werden Sie aufgefordert, die Zertifikate auf den CSM-Server hochzuladen. Das Dienstprogramm zeigt einen Fehler an: • Wenn die Eingabeblöcher nicht im erforderlichen Format vorliegen • Wenn das Zertifikatsdatum ungültig ist oder das Zertifikat bereits abgelaufen ist. • Wenn das Serverzertifikat nicht überprüft oder auf ein Stammzertifikat der Zertifizierungsstelle zurückverfolgt werden konnte. • Wenn eine der Zwischenzertifikate nicht als Eingabe angegeben wurde. • Wenn der private Schlüssel des Servers fehlt oder das hochgeladene Serverzertifikat nicht mit dem privaten Schlüssel des Servers verifiziert werden konnte. Sie müssen sich an die Zertifizierungsstelle wenden, die die Zertifikate ausgestellt hat, um diese Probleme zu beheben, bevor Sie die Zertifikate in den CSM hochladen.
5	Hochladen eines einzelnen Serverzertifikats zum Server	Sie müssen die Zertifikate mit Option 4 überprüfen, bevor Sie diese Option auswählen.

		Wählen Sie diese Option nur aus, wenn keine Zwischenzertifikate vorhanden sind und nur das Serverzertifikat durch ein prominentes Root CA-Zertifikat signiert ist. Wenn die Root-CA von CSM nicht als vertrauenswürdig eingestuft wird, wählen Sie diese Option nicht aus. In diesem Fall müssen Sie ein Zertifikat für die Stammzertifizierungsstelle zum Signieren des Zertifikats von der Zertifizierungsstelle erhalten und beide Zertifikate mit Option 6 hochladen. Wenn Sie diese Option auswählen und den Speicherort des Zertifikats angeben, kann das Dienstprogramm: • Überprüft, ob das Zertifikat im Base64-Format mit verschlüsseltem X.509-Zertifikat vorliegt. • Zeigt den Gegenstand des Zertifikats und die Einzelheiten des Zertifikats an. • Überprüft, ob das Zertifikat auf dem Server gültig ist. • Überprüft, ob der private Schlüssel des Servers und das Zertifikat des Eingabeservers übereinstimmen. • Überprüft, ob das Serverzertifikat auf das für die Signierung verwendete Root-Zertifizierungsstellenzertifikat zurückverfolgt werden kann. Nach erfolgreicher Überprüfung lädt das Dienstprogramm das Zertifikat auf CiscoWorks Server hoch. Das Dienstprogramm zeigt einen Fehler an: • Wenn die Eingabeblöcher nicht im erforderlichen Format vorliegen • Wenn das Zertifikatsdatum ungültig ist oder das Zertifikat bereits abgelaufen ist. • Wenn das Serverzertifikat nicht überprüft oder auf ein Stammzertifikat der Zertifizierungsstelle zurückverfolgt werden konnte. • Wenn der private Schlüssel des Servers fehlt oder das hochgeladene Serverzertifikat nicht mit dem privaten Schlüssel des Servers verifiziert werden konnte. Sie müssen sich an die Zertifizierungsstelle wenden, die die Zertifikate ausgestellt hat, um diese Probleme zu beheben, bevor Sie die Zertifikate erneut in CSM hochladen.
6	Hochladen einer Zertifikatskette auf	Sie müssen die Zertifikate mit Option 4

Server	überprüfen, bevor Sie diese Option auswählen. Wählen Sie diese Option aus, wenn Sie eine Zertifikatskette hochladen. Wenn Sie auch das Root-Zertifizierungsstellenzertifikat hochladen, müssen Sie es als eines der Zertifikate in der Kette einschließen. Wenn Sie diese Option auswählen und den Speicherort der Zertifikate angeben, kann das Dienstprogramm Folgendes ausführen: • Überprüft, ob das Zertifikat im Base64-Format mit verschlüsseltem X.509-Zertifikat vorliegt. • Zeigt den Gegenstand des Zertifikats und die Einzelheiten des Zertifikats an. • Überprüft, ob das Zertifikat auf dem Server gültig ist • Überprüft, ob der private Serverschlüssel und das Serverzertifikat übereinstimmen. • Überprüft, ob das Serverzertifikat auf das Stammzertifikat der Zertifizierungsstelle zurückverfolgt werden kann, das für die Signierung verwendet wurde. • Erstellt die Zertifikatskette, wenn Zwischenketten angegeben werden, und überprüft, ob die Kette mit dem entsprechenden Stammzertifikat der Zertifizierungsstelle endet. Nach erfolgreicher Überprüfung wird das Serverzertifikat auf CiscoWorks Server hochgeladen. Alle Zwischenzertifikate und das Zertifikat der Stammzertifizierungsstelle werden hochgeladen und in den CSM TrustStore kopiert. Das Dienstprogramm zeigt einen Fehler an: • Wenn die Eingabeblöcher nicht im erforderlichen Format vorliegen. • Wenn das Zertifikatsdatum ungültig ist oder das Zertifikat bereits abgelaufen ist. • Wenn das Serverzertifikat nicht überprüft oder auf ein Stammzertifikat der Zertifizierungsstelle zurückverfolgt werden konnte. • Wenn eine der Zwischenzertifikate nicht als Eingabe angegeben wurde. • Wenn der private Schlüssel des Servers fehlt oder das hochgeladene Serverzertifikat nicht mit dem privaten Schlüssel des Servers verifiziert werden

		konnte.
7	Zertifikat für allgemeine Dienste ändern	Sie müssen sich an die Zertifizierungsstelle wenden, die die Zertifikate ausgestellt hat, um diese Probleme zu beheben, bevor Sie die Zertifikate erneut in CiscoWorks hochladen. Mit dieser Option können Sie den Eintrag Hostname im Zertifikat für allgemeine Dienste ändern. Sie können einen alternativen Hostnamen eingeben, wenn Sie den vorhandenen Hostnamen ändern möchten.



Schritt 2 Verwenden Sie **Option 1**, um eine Kopie des aktuellen Zertifikats abzurufen und es als zukünftige Referenz zu speichern.

Schritt 3 Beenden Sie den CSM-Daemon-Manager mit diesem Befehl an der Windows-Eingabeaufforderung, bevor Sie den Prozess zum Hochladen von Zertifikaten starten.

```
net stop crmdmgtd
```

> **Hinweis**: Mit diesem Befehl werden die CSM-Dienste deaktiviert. Stellen Sie sicher, dass während dieses Verfahrens keine Bereitstellungen aktiv sind.

Schritt 4 Öffnen Sie das SSL-Dienstprogramm erneut. Dieses Dienstprogramm kann mithilfe der Eingabeaufforderung geöffnet werden, indem Sie zum zuvor erwähnten Pfad navigieren und diesen Befehl verwenden.

```
perl SSLUtil.pl
```

Schritt 5 Wählen Sie **Option 4 aus**. **Überprüfen Sie die Zertifikatskette für die Eingabe.**

Schritt 6 Geben Sie den Speicherort der Zertifikate ein (Serverzertifikat und Zwischenzertifikat).

> **Hinweis**: Das Skript überprüft, ob das Serverzertifikat gültig ist. Nach Abschluss der Überprüfung zeigt das Dienstprogramm die Optionen an. Wenn das Skript während der

Validierung und Überprüfung Fehler meldet, werden im SSL-Dienstprogramm Anweisungen zum Korrigieren dieser Fehler angezeigt. Befolgen Sie die Anweisungen, um diese Probleme zu beheben, und versuchen Sie die gleiche Option noch einmal.

Schritt 7 Wählen Sie eine der nächsten beiden Optionen aus.

Wählen Sie **Option 5** aus, wenn nur ein Zertifikat hochgeladen werden soll, d. h. wenn das Serverzertifikat durch ein Zertifikat der Stammzertifizierungsstelle signiert ist.

ODER

Wählen Sie **Option 6 aus**, wenn eine Zertifikatskette hochgeladen wird, d. h. wenn ein Serverzertifikat und ein Zwischenzertifikat vorhanden sind.

Hinweis: CiscoWorks lässt den Upload nicht zu, wenn der CSM Daemon Manager nicht angehalten wurde. Das Dienstprogramm zeigt eine Warnmeldung an, wenn im hochgeladenen Serverzertifikat falsche Hostnamen festgestellt wurden, der Upload jedoch fortgesetzt werden kann.

Schritt 8 Geben Sie die erforderlichen Details ein.

- Ort des Zertifikats
- Ort der ggf. Zwischenzertifikate.

SSL Utility lädt die Zertifikate hoch, wenn alle Details korrekt sind und die Zertifikate die CSM-Anforderungen für Sicherheitszertifikate erfüllen.

Schritt 9 Starten Sie den CSM Daemon Manager neu, damit die neue Änderung wirksam wird und die CSM-Dienste aktiviert werden.

```
net start crmdmgtd
```

Hinweis: Warten Sie insgesamt 10 Minuten, bis alle CSM-Dienste neu gestartet werden.

Schritt 10 Bestätigen Sie, dass der CSM das installierte Identitätszertifikat verwendet.

Hinweis: Vergessen Sie nicht, die Root- und Zwischenzertifikate der Zertifizierungsstellen auf dem PC oder Server zu installieren, von dem aus die SSL-Verbindung zum CSM hergestellt wird.