

Identity Services Engine - Misstrauen gegenüber den Behörden für Ausweis- und Zwischenzertifikate im Notfall

Inhalt

Zweck

Im Folgenden finden Sie die Richtlinien zur Identity Services Engine und ISE PIC (Passive Identity Connector) für das Misstrauen der Behörden für Ausstellungs- und Zwischenzertifikate in Notfällen. Die Konfiguration der Identity Service Engine umfasst standardmäßig nicht die betroffenen Mudhra Root- und Intermediate Certificate-Behörden im Trusted Store. Die ISE-Konfiguration sollte jedoch überprüft werden, um sicherzustellen, dass sie nach der Installation nicht verwendet werden.

HAFTUNGSAUSSCHLUSS

Dieser Artikel dient nur dazu, die ISE-Konfiguration auf das Vorhandensein der betroffenen Zertifizierungsstellen zu überprüfen. Die Identity Services Engine als Ganzes wird derzeit noch untersucht und erfordert möglicherweise in Zukunft weitere Konfigurationen oder Software-Updates. Dieser Artikel wird zusammen mit der Sicherheitsempfehlung unter <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r> aktualisiert.

Systemzertifikate

Navigieren Sie zu Administration -> System -> Zertifikate -> Systemzertifikate, wählen Sie jedes den Knoten 1 von 1 zugewiesene Zertifikat aus, und wählen Sie Ansicht aus. [1]



Certificate Hierarchy

Certificate Services Root CA - zer0k-ise1

Certificate Services Node CA - zer0k-ise1

Certificate Services Endpoint Sub CA - zer0k-ise1

zer0k-ise1.zer0k.org



zer0k-ise1.zer0k.org

Issued By : Certificate Services Endpoint Sub CA - zer0k-ise1

Expires : Mon, 4 Aug 2031 10:52:08 EDT

Certificate status is good

Details

Issued To

Common Name (CN) zer0k-ise1.zer0k.org

Stellen Sie sicher, dass die betroffenen Zertifizierungsstellen oder ausstellenden Zertifikate nicht in der Zertifikathierarchie enthalten sind. Wenn der Service verwendet wird, beginnen Sie mit der Migration des Service zu einer neuen Zertifizierungsstelle.

Vertrauenswürdige Zertifikate

Navigieren Sie zu Administration -> System -> Certificates -> Trusted Certificates (Verwaltung -> System -> Zertifikate -> Vertrauenswürdige Zertifikate), und überprüfen Sie die Liste der installierten Root- und Zwischenzertifikate. Wenn Sie eine oder mehrere der betroffenen CAs in der Liste "Vertrauenswürdige" finden, notieren Sie sich die Spalte "Vertrauenswürdige für", und führen Sie für jeden Typ [2] die folgenden Schritte aus:

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From
		Endpoints				
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016
☐	Cisco Root CA M1	Infrastructure Cisco Services Endpoints AdminAuth NativeIPSec	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 20...

- Cisco Services - Cisco verwendet Mudhura nicht für Services. Wenn dies der einzige Eintrag ist, kann das Zertifikat gelöscht werden.
- Infrastruktur - Stellen Sie sicher, dass die Rolle "Endpoints" und/oder "AdminAuth" nicht erforderlich ist. Stellen Sie sicher, dass unter "Systemzertifikate" kein Zertifikat der Zertifizierungsstelle oder von den Ausstellern verwendet wird.
- Endpunkte: Überprüfen Sie, ob die Endpunkte authentifiziert werden müssen und die kompromittierte Kette erforderlich ist. Wenn Sie sich nicht sicher sind, ob die Endpunkte die CA oder die Issuers verwenden, deaktivieren Sie die Option "Trust for client authentication and Syslog" (Für Client-Authentifizierung und Syslog vertrauen), und überwachen Sie Live-Protokolle und Berichte, wenn bei der Client-Authentifizierung Fehler auftreten.
- AdminAuth - Geben Sie neue Zertifikate an Ihre Administratoren, als schnelle Option Admin Authentication kann zurück auf Passwort-basierte Anmeldung, während neue Zertifikate ausgegeben werden verschoben werden.
- NativeIPSec - Bei Verwendung der Native IPSec-Funktion sollten die IPSec-Clients auf eine neue CA migriert werden.

Weitere Services

Die folgenden Dienstkonfigurationen sollten überprüft werden, um sicherzustellen, dass das Löschen der betroffenen vertrauenswürdigen Zertifikate keine Auswirkungen auf die Funktion des Systems hat. Wenn diese Dienste verwendet werden, müssen die Dienste so umkonfiguriert werden, dass sie neue Zertifikate verwenden, bevor die vertrauenswürdigen Zertifikate gelöscht werden.

LSAP

Navigieren Sie zu Administration -> Identity Management -> External Identity Sources -> LDAP. Klicken Sie unter jedem LDAP-Eintrag auf die Registerkarte Verbindung. Wenn die sichere Authentifizierung aktiviert ist, überprüfen Sie die Kette für die Einstellungen "LDAP-Server-Stammzertifizierungsstelle" und "Ausstellerzertifizierungsstelle der ISE". [3]

LDAP Server Root CA	VeriSign Class 3 Public Priv	LDAP Server Root CA	VeriSign Class 3 Public Priv
Issuer CA of ISE Certificates	DigiCert Global Root CA	Issuer CA of ISE Certificates	Select if required (optional)

SYSLOG

Navigieren Sie zu Administration -> System -> Logging -> Remote Logging Targets, zeigen Sie jeden konfigurierten Secure SYSLOG Server für das konfigurierte Trusted Root-Zertifikat an. Wenn eines der betroffenen CA-Zertifikate verwendet wird, überprüfen Sie die Kette auf dem SYSLOG-Server und stellen Sie ggf. einen neuen Root aus, und vertrauen Sie ihm. [4]

Select CA Certificate

Cisco Root CA M1

Note: The CA certificates should be imported into the Certificate Store, enabled, and trusted for client authentication prior to configuring Secure Syslog. Ensure that a local certificate signed by the selected CA exists on the primary and secondary nodes.

If a local certificate signed by the selected CA does not exist, the self-signed local certificate will be used.

Ignore Server Certificate validation ☐

RADIUS-DTLS

Optional kann unter jedem Netzwerkgerät unter Administration -> Network Resources -> Network Devices die "Issuer CA of ISE Certificates for CoA" (Ausstellerzertifizierung für CoA) festgelegt werden. Diese Einstellung wird nur verwendet, um das Client-Zertifikat auszuwählen, das die ISE verwendet, um eine CoA an ein für DTLS konfiguriertes Netzwerkgerät auszugeben. Das Zertifikat wird für den Knoten auf der Seite "Systemzertifikate" in ISE angezeigt. Diese Einstellung muss daher nur für jedes konfigurierte Netzwerkgerät überprüft werden, wenn ein Zertifikatproblem mit einem der Mudhra-Zertifikate für einen ISE-Knoten ausgegeben wird.

[1] [Zertifikatsverwaltung in der ISE](#)

[2] [Einstellungen für vertrauenswürdige ISE-Zertifikate](#)

[3] [Sichere LDAP-Konfiguration der ISE](#)

[4] [Konfigurieren eines sicheren Syslog-Remote-Protokollierungsziels](#)

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.