Konfigurieren von Chiffren in ISE 3.3 und höher

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die verschiedenen, von ISE 3.3 und höher in verschiedenen Services verwendeten Chiffren ändern können, sodass der Benutzer die Kontrolle über diese Mechanismen hat.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponente

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Unterstützte Cipher Suites

Die Cisco ISE unterstützt die TLS-Versionen 1.0, 1.1 und 1.2.

Ab Cisco ISE Version 3.3 wurde TLS 1.3 nur für die Administrations-GUI eingeführt. Diese Verschlüsselungen werden für den Admin-HTTPS-Zugriff über TL 1.3 unterstützt:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

- TLS_CHACHA20_POLY1305_SHA256

Die Cisco ISE unterstützt RSA- und ECDSA-Serverzertifikate. Diese elliptischen Kurven werden unterstützt:

- Secp256r1
- Secp384r1
- Secp521r1

In dieser Tabelle sind die unterstützten Cipher Suites aufgeführt:

Cipher-Suite	EAP-Authentifizierung/RADIUS DTLS	CRL-Download über HTTPS oder Secure LDAP/Secure Syslog Communication/DTLS CoA
ECDHE-ECDSA-AES256-GCM-SHA384	Ja, wenn TLS 1.1 zulässig ist.	Ja, wenn TLS 1.1 zulässig ist.
ECDHE-ECDSA-AES128-GCM-SHA256	Ja, wenn TLS 1.1 zulässig ist.	Ja, wenn TLS 1.1 zulässig ist.
ECDHE-ECDSA-AES256-SHA384	Ja, wenn TLS 1.1 zulässig ist.	Ja, wenn TLS 1.1 zulässig ist.
ECDHE-ECDSA-AES128-SHA256	Ja, wenn TLS 1.1 zulässig ist.	Ja, wenn TLS 1.1 zulässig ist.
ECDHE-ECDSA-AES256-SHA	Ja, wenn SHA-1 zulässig ist.	Ja, wenn SHA-1 zulässig ist.
ECDHE-ECDSA-AES128-SHA	Ja, wenn SHA-1 zulässig ist.	Ja, wenn SHA-1 zulässig ist.
ECDHE-RSA-AES256-GCM-SHA384	Ja, wenn ECDHE-RSA erlaubt ist.	Ja, wenn ECDHE-RSA zulässig ist.
ECDHE-RSA-AES128-GCM-SHA256	Ja, wenn ECDHE-RSA erlaubt ist.	Ja, wenn ECDHE-RSA erlaubt ist.
ECDHE-RSA-AES256-SHA384	Ja, wenn ECDHE-RSA erlaubt	Ja, wenn ECDHE-RSA erlaubt

	ist.	ist.
ECDHE-RSA-AES128-SHA256	Ja, wenn ECDHE-RSA erlaubt ist.	Ja, wenn ECDHE-RSA erlaubt ist.
ECDHE-RSA-AES256-SHA	Ja, wenn ECDHE-RSA/SHA-1 zulässig ist.	Ja, wenn ECDHE-RSA/SHA-1 zulässig ist.
ECDHE-RSA-AES128-SHA	Ja, wenn ECDHE-RSA/SHA-1 zulässig ist.	Ja, wenn ECDHE-RSA/SHA-1 zulässig ist.
DHE-RSA-AES 256-SHA 256	Nein	Ja
DHE-RSA-AES 128-SHA 256	Nein	Ja
DHE-RSA-AES256-SHA	Nein	Ja, wenn SHA-1 zulässig ist.
DHE-RSA-AES128-SHA	Nein	Ja, wenn SHA-1 zulässig ist.
AES 256-SHA 256	Ja	Ja
AES 128-SHA 256	Ja	Ja
AES 256 SHA	Ja, wenn SHA-1 zulässig ist.	Ja, wenn SHA-1 zulässig ist.
AES-128 SHA	Ja, wenn SHA-1 zulässig ist.	Ja, wenn SHA-1 zulässig ist.
DES-CBC-SHA	Ja, wenn 3DES/SHA-1 zulässig ist.	Ja, wenn 3DES/SHA-1 zulässig ist.
DHE-DSS-AES256-SHA	Nein	Ja, wenn 3DES/DSS und SHA-1 aktiviert sind.
DHE-DSS-AES128-SHA	Nein	Ja, wenn 3DES/DSS und SHA-1 aktiviert sind.

EDH-DSS-DES-CBC3-SHA	Nein	Ja, wenn 3DES/DSS und SHA-1 aktiviert sind.
RC4-SHA	Wenn die Option Schwache Chiffren zulassen auf der Seite Zulässige Protokolle aktiviert ist und wenn SHA-1 zulässig ist.	Nein
RC4-MD5	Wenn die Option Schwache Chiffren zulassen auf der Seite Zulässige Protokolle aktiviert ist und wenn SHA-1 zulässig ist.	Nein
Nur anonyme AP-FAST-Bereitstellung: ADH-AES-128-SHA	Ja	Nein
Schlüsselverwendung überprüfen	Das Clientzertifikat kann KeyUsage=Key Agreement und ExtendedKeyUsage=Client Authentication für diese Chiffren enthalten: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validierung der ExtendedKeyUsage	Das Clientzertifikat muss KeyUsage=Key Encipherment und ExtendedKeyUsage=Client Authentication für diese Chiffren aufweisen: • AES 256-SHA 256 • AES 128-SHA 256 • AES 256 SHA • AES-128 SHA • DHE-RSA-AES128-SHA	Das Serverzertifikat muss über ExtendedKeyUsage=Server Authentication verfügen.

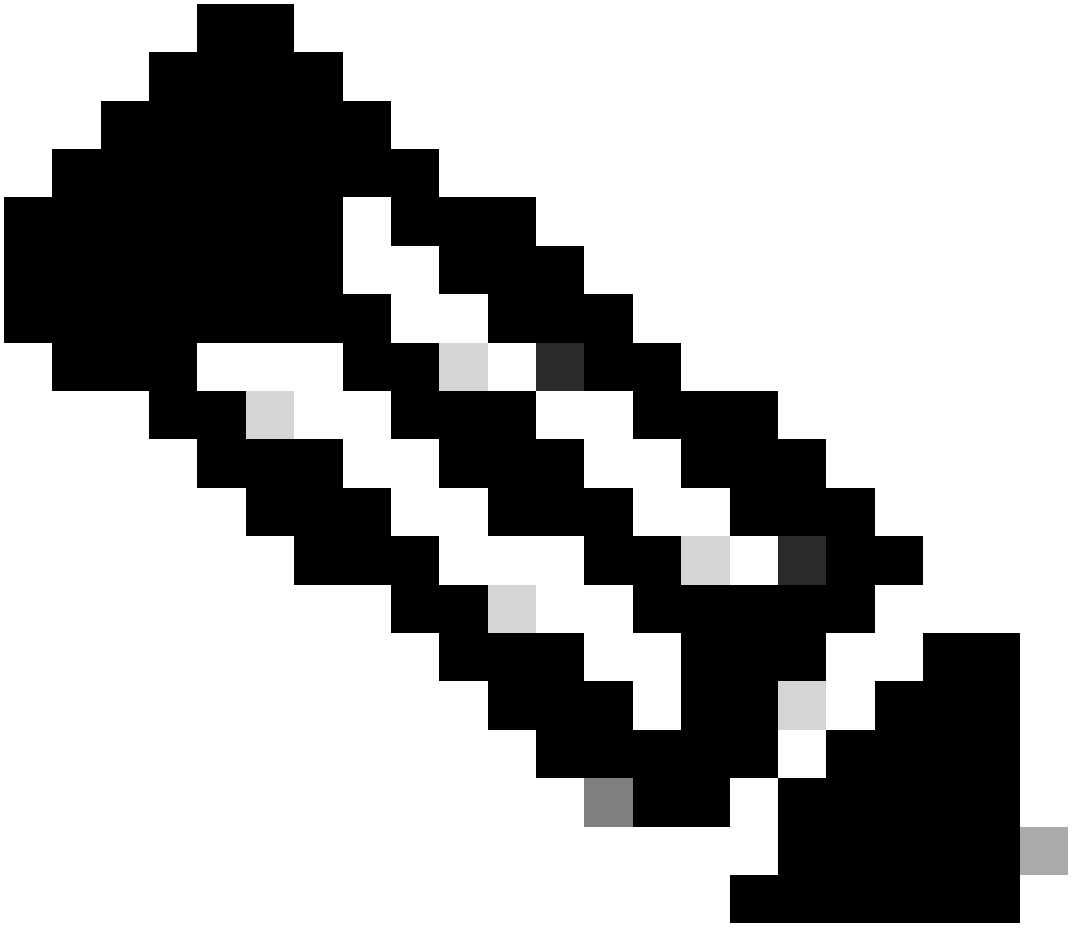
Konfigurationen

Sicherheitseinstellungen konfigurieren

Gehen Sie folgendermaßen vor, um die Sicherheitseinstellungen zu konfigurieren:

1. Klicken Sie in der Cisco ISE-GUI auf das Menüsymbol (), und wählen Sie Administration > System > Settings > Security Settings (Verwaltung > System > Einstellungen > Sicherheitseinstellungen) aus.

2. Wählen Sie im Abschnitt TLS-Versionseinstellungen eine oder mehrere aufeinander folgende TLS-Versionen aus. Aktivieren Sie das Kontrollkästchen neben den TLS-Versionen, die Sie aktivieren möchten.



Hinweis: TLS 1.2 ist standardmäßig aktiviert und kann nicht deaktiviert werden. Wenn Sie mehr als eine TLS-Version auswählen, müssen Sie aufeinander folgende Versionen auswählen. Wenn Sie beispielsweise TLS 1.0 auswählen, wird TLS 1.1 automatisch aktiviert. Wenn Sie die Chiffren hier ändern, kann die ISE neu gestartet werden.

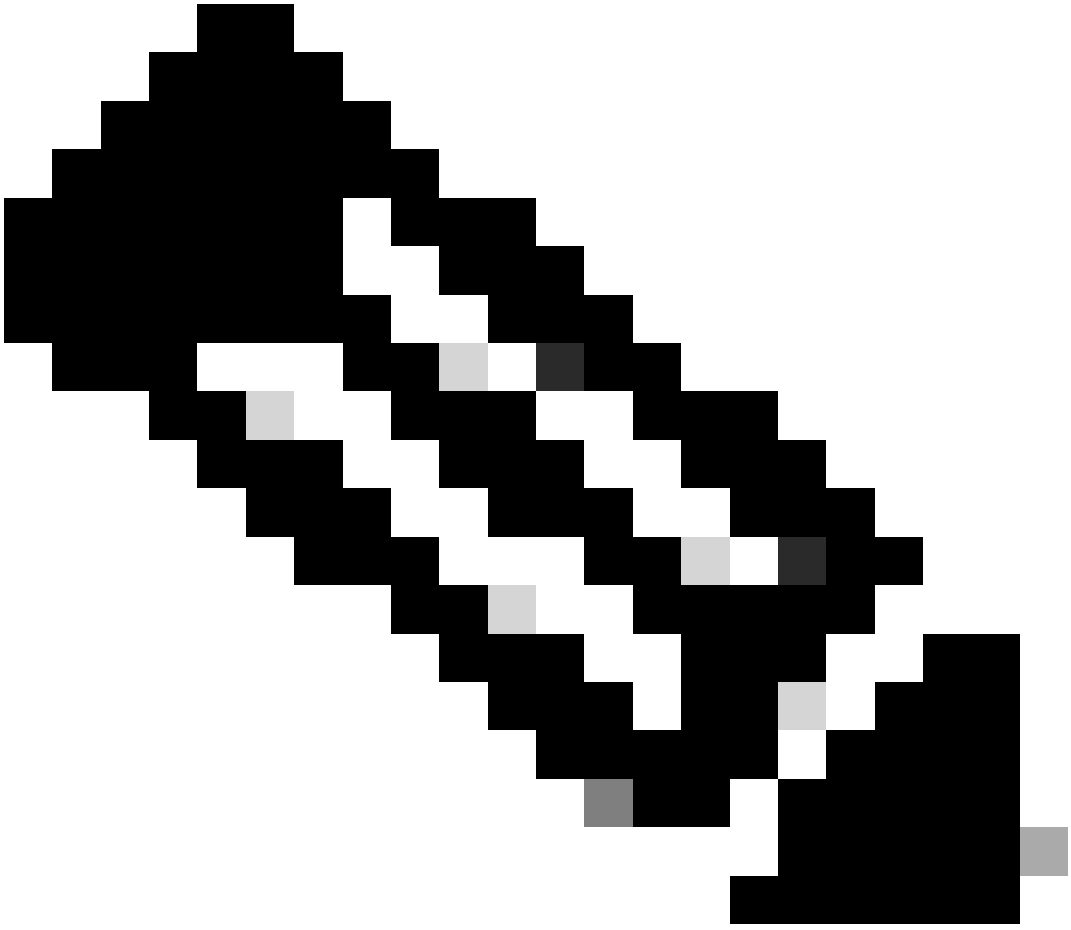
TLS 1.0, 1.1 und 1.2 zulassen: Aktiviert TLS 1.0, 1.1 und 1.2 für die nächsten Services. Außerdem SHA-1-Chiffren zulassen: Ermöglicht SHA-1-Chiffren die Kommunikation mit Peers für diese Workflows:

- EAP-Authentifizierung.
- Sperrlisten vom HTTPS-Server herunterladen.
- Sichere Syslog-Kommunikation zwischen der ISE und dem externen Syslog-Server
- ISE als sicherer LDAP-Client.
- ISE als sicherer ODBC-Client.
- ERS-Services.
- pxGrid-Services.
- Alle ISE-Portale (z. B. Guest Portal, Client Provisioning Portal, MyDevices Portal).

- MDM-Kommunikation:
- PassiveID-Agent-Kommunikation.
- Bereitstellung durch die Zertifizierungsstelle.
- Administrator-GUI-Zugriff.

Diese Ports werden von den oben aufgeführten Komponenten für die Kommunikation verwendet:

- Administratorzugriff: 443
- Cisco ISE-Portale: 9002, 8443, 8444, 8445, 8449 oder alle für ISE-Portale konfigurierten Ports
- ERS: 9060, 9061, 9063
- pxGrid: 8910



Hinweis: Die Option SHA-1-Chiffren zulassen ist standardmäßig deaktiviert. Wir empfehlen die Verwendung von SHA-256- oder SHA-384-Chiffren zur Erhöhung der Sicherheit.

Sie müssen alle Knoten in einer Bereitstellung neu starten, nachdem Sie die Option SHA-1-Chiffren zulassen aktiviert oder deaktiviert haben. Wenn der Neustart nicht erfolgreich ist, werden die Konfigurationsänderungen nicht angewendet.

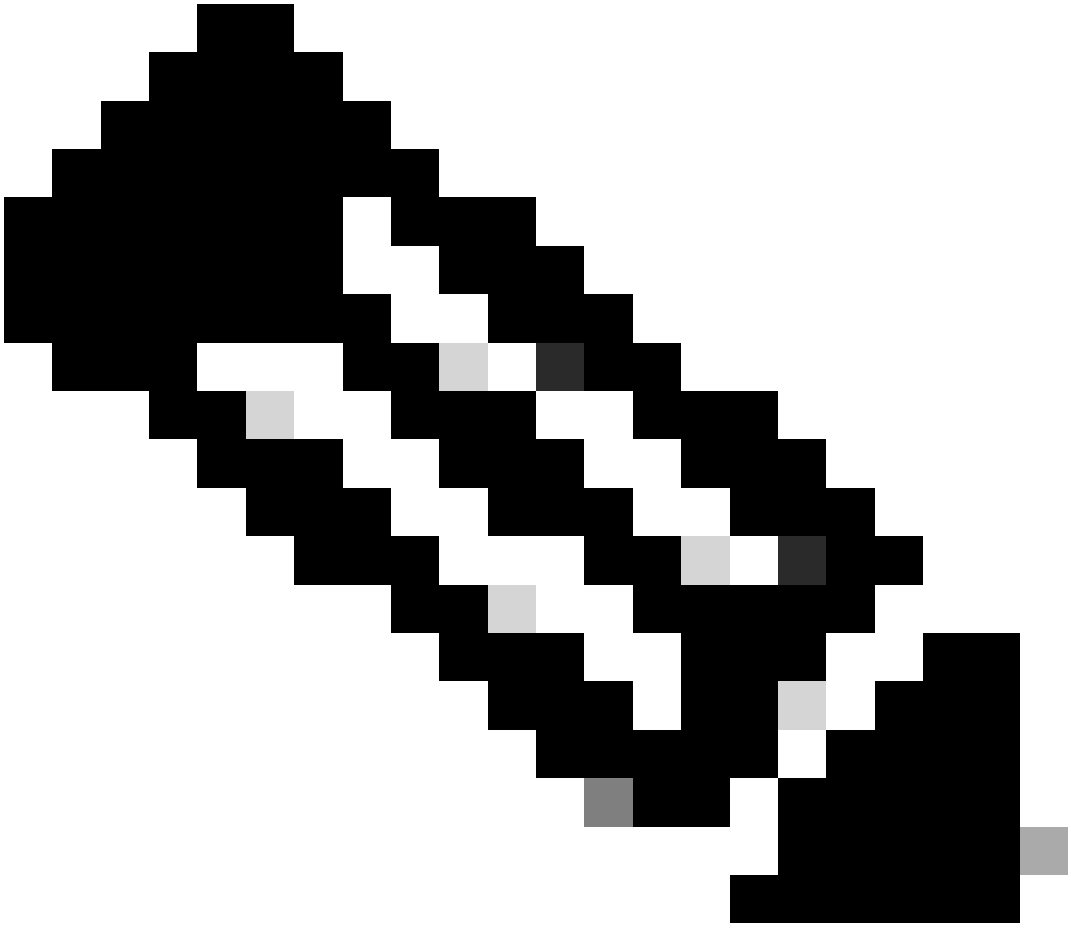
Wenn die Option SHA-1-Chiffren zulassen deaktiviert ist und ein Client mit nur SHA-1-Chiffren versucht, eine Verbindung mit der Cisco ISE herzustellen, schlägt der Handshake fehl, und im Client-Browser wird eine Fehlermeldung angezeigt.

Wählen Sie eine der Optionen aus, während SHA-1-Chiffren mit Legacy-Peers kommunizieren können:

- Alle SHA-1-Verschlüsselungen zulassen: Ermöglicht allen SHA-1-Verschlüsselungen die Kommunikation mit älteren Peers.
- Nur TLS_RSA_WITH_AES_128_CBC_SHA zulassen: Nur TLS_RSA_WITH_AES_128_CBC_SHA-Chiffre kann mit Legacy-Peers kommunizieren.

TLS 1.3 zulassen: TLS 1.3 für Administrator-HTTPS-Zugriff über Port 443 für:

- Cisco ISE-Administrations-GUI
- APIs aktiviert für Port 443 (offene API, ERS, MnT)



Hinweis: AAA-Kommunikation und alle Arten von Internode-Kommunikation unterstützen TLS 1.3 nicht. Aktivieren Sie TLS 1.3 auf der Cisco ISE und den relevanten Clients und Servern für den Administratorzugriff über TLS 1.3.

ECDHE-RSA- und 3DES-Verschlüsselung zulassen: Ermöglicht die Kommunikation zwischen ECDHE-RSA-Verschlüsselungen und Peers für diese Workflows:

- Die Cisco ISE ist als EAP-Server konfiguriert
- Die Cisco ISE ist als RADIUS-DTLS-Server konfiguriert.
- Die Cisco ISE ist als RADIUS DTLS-Client konfiguriert.
- Cisco ISE lädt Zertifikatsperrliste von HTTPS oder einem sicheren LDAP-Server herunter
- Die Cisco ISE ist als sicherer Syslog-Client konfiguriert.
- Die Cisco ISE ist als sicherer LDAP-Client konfiguriert.

DSS-Chiffren für ISE als Client zulassen: Wenn die Cisco ISE als Client fungiert, können DSS-Chiffren mit einem Server für folgende Workflows kommunizieren:

- Die Cisco ISE ist als RADIUS DTLS-Client konfiguriert.
- Cisco ISE lädt Zertifikatsperrliste von HTTPS oder einem sicheren LDAP-Server herunter
- Die Cisco ISE ist als sicherer Syslog-Client konfiguriert.
- Die Cisco ISE ist als sicherer LDAP-Client konfiguriert.

Unsichere Legacy-TLS-Neuaushandlung für ISE als Client zulassen: Ermöglicht die Kommunikation mit Legacy-TLS-Servern, die eine sichere TLS-Neuaushandlung für diese Workflows nicht unterstützen:

- Cisco ISE lädt Zertifikatsperrliste von HTTPS oder einem sicheren LDAP-Server herunter
- Die Cisco ISE ist als sicherer Syslog-Client konfiguriert.
- Die Cisco ISE ist als sicherer LDAP-Client konfiguriert.

Ungültige Benutzernamen angeben: Cisco ISE zeigt standardmäßig die ungültige Meldung für Authentifizierungsfehler aufgrund falscher Benutzernamen an. Um das Debugging zu vereinfachen, erzwingt diese Option, dass die Cisco ISE Benutzernamen in Berichten und nicht die ungültige Meldung anzeigt. Beachten Sie, dass Benutzernamen immer für fehlgeschlagene Authentifizierungen angezeigt werden, die nicht auf falsche Benutzernamen zurückzuführen sind.

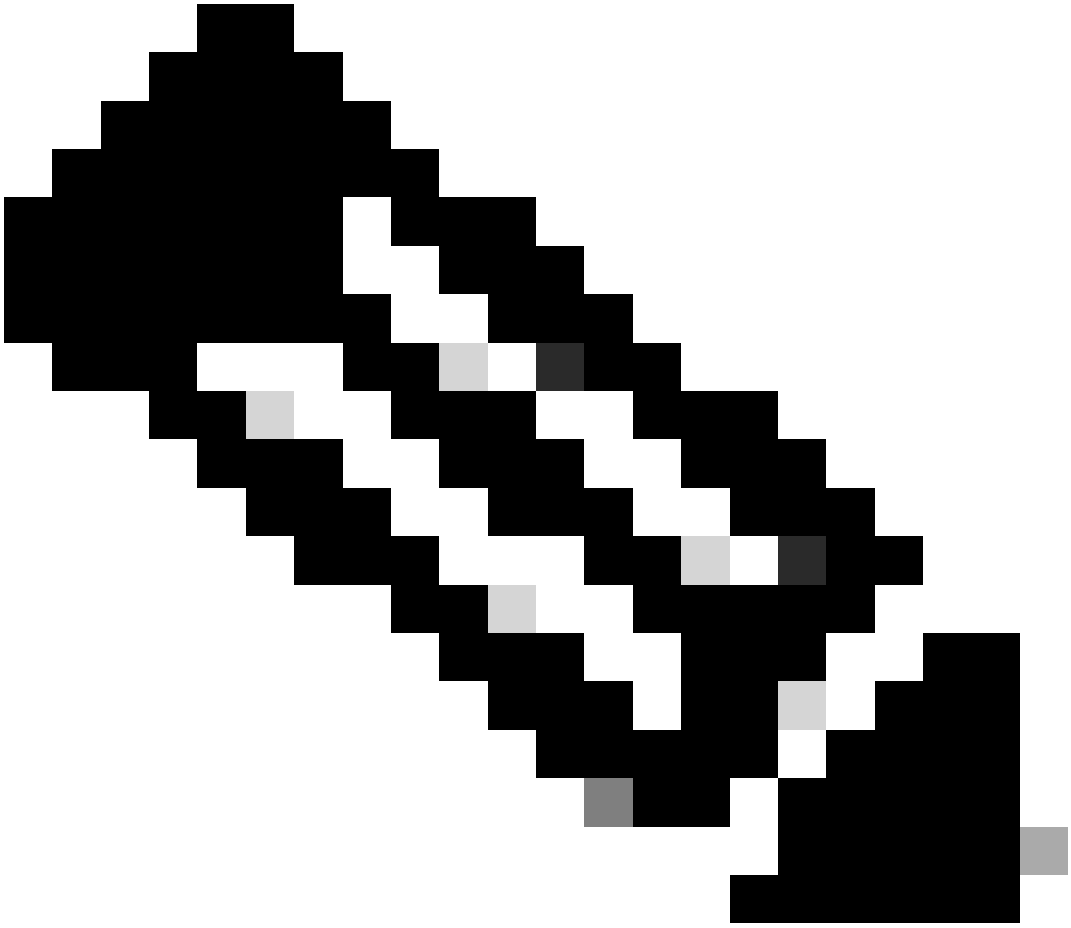
Diese Funktion wird für Active Directory-, interne Benutzer-, LDAP- und ODBC-Identitätsquellen unterstützt. Sie wird für andere Identitätsquellen wie RADIUS-Token, RSA oder SAML nicht unterstützt.

FQDN-basierte Zertifikate für die Kommunikation mit Drittanbietern (TC-NAC) verwenden: FQDN-basierte Zertifikate müssen folgende Regeln erfüllen:

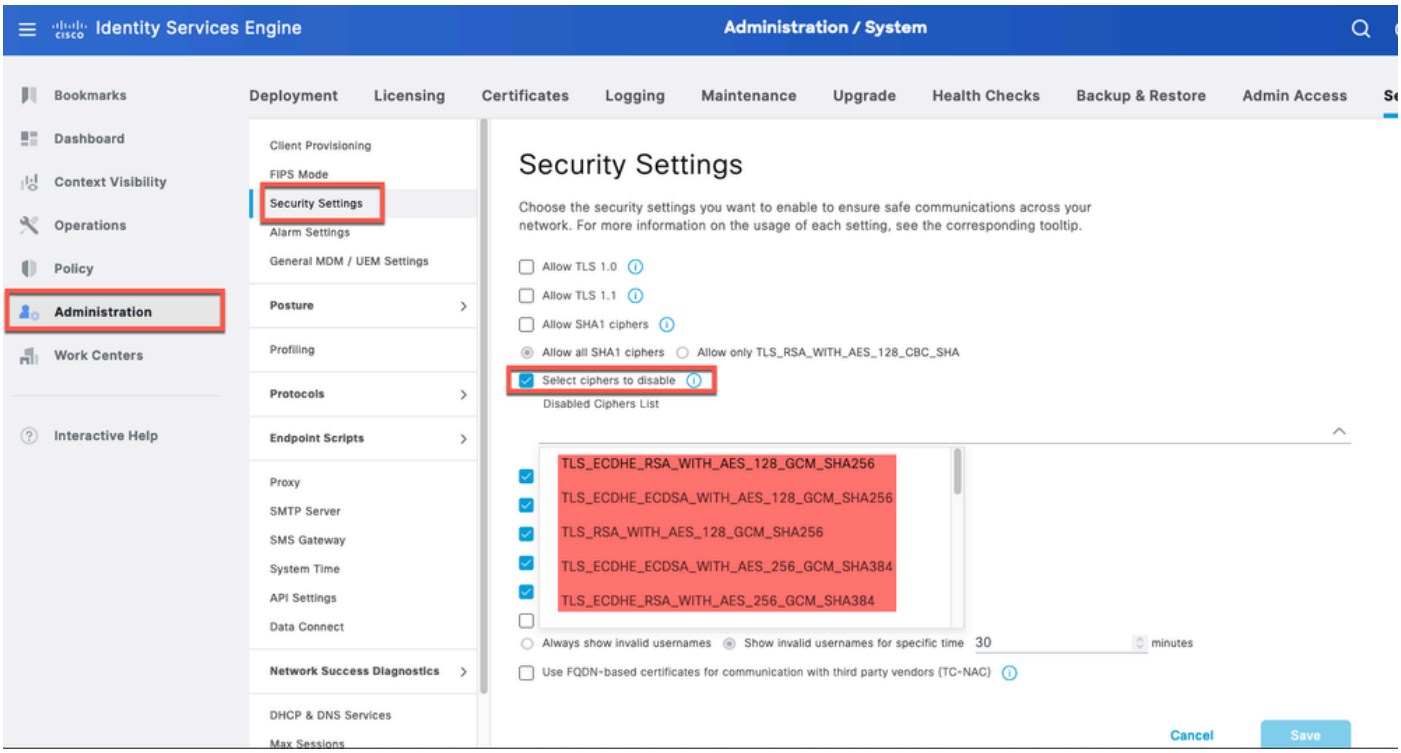
- Die SAN- und CN-Felder im Zertifikat müssen FQDN-Werte enthalten. Hostnamen und IP-Adressen werden nicht unterstützt.
- Platzhalterzertifikate dürfen den Platzhalter nur im äußersten linken Fragment enthalten.
- Der in einem Zertifikat bereitgestellte FQDN muss DNS-auflösbar sein.

Spezifische Chiffren deaktivieren

Aktivieren Sie die Option Ciphers List manuell konfigurieren, wenn Sie die Verschlüsselung manuell für die Kommunikation mit den folgenden Cisco ISE-Komponenten konfigurieren möchten: Admin-UI, ERS, OpenAPI, sicheres ODBC, Portale und pxGrid. Es wird eine Liste mit zulässigen Chiffren angezeigt. Wenn z. B. die Option SHA1-Chiffren zulassen aktiviert ist, werden SHA1-Chiffren in dieser Liste aktiviert. Wenn die Option Nur TLS_RSA_WITH_AES_128_CBC_SHA zulassen aktiviert ist, wird nur dieser SHA1-Verschlüsselungscode in dieser Liste aktiviert. Wenn die Option SHA1-Chiffren zulassen deaktiviert ist, können Sie hier keine SHA1-Chiffren aktivieren.

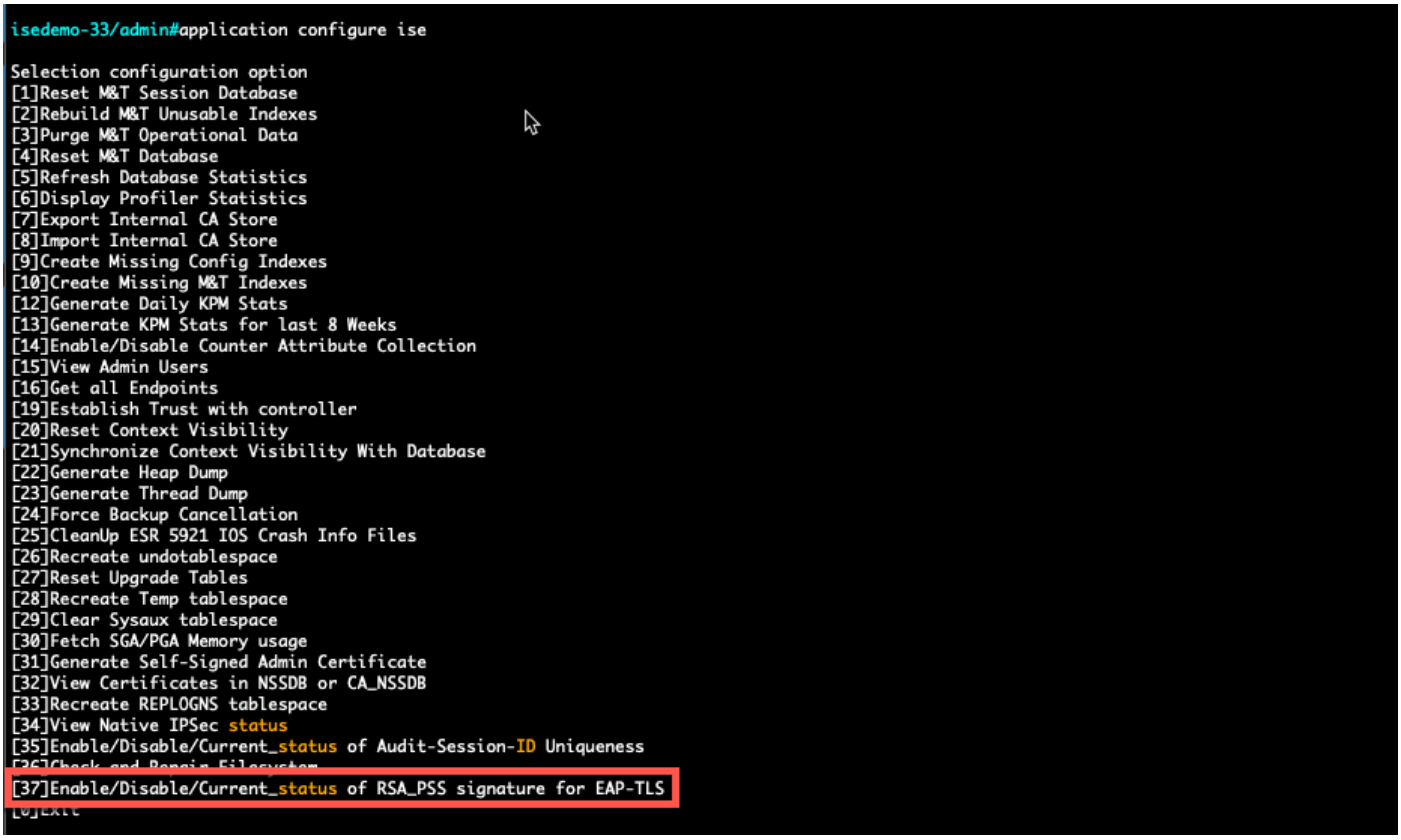


Hinweis: Wenn Sie die Liste der zu deaktivierenden Chiffren bearbeiten, startet der Anwendungsserver auf allen Cisco ISE-Knoten neu. Wenn der FIPS-Modus aktiviert oder deaktiviert ist, werden die Anwendungsserver auf allen Knoten neu gestartet, was zu erheblichen Systemausfällen führt. Wenn Sie mit der Option "Ciphers List manuell konfigurieren" Chiffren deaktiviert haben, überprüfen Sie die Liste der deaktivierten Chiffren, nachdem die Anwendungsserver neu gestartet wurden. Die Liste der deaktivierten Chiffren wird aufgrund des Übergangs in den FIPS-Modus nicht geändert.



Option zum Deaktivieren von Ciphers ISE 3.3

- Über die ISE-CLI können Sie den Befehl ausführen application configure iseund die Option 37 verwenden, die in diesem Screenshot hervorgehoben ist: **Enable/Disable/Current_status der RSA_PSS-Signatur für EAP-TLS**. Der zugehörige Fehler ist die Cisco Bug-ID CSCwb77915.



Option zum Deaktivieren/Aktivieren von RSA_PSS für EAP-TLS

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.