Configurazione delle cifrature in ISE 3.3 e versioni successive

Sommario

Introduzione

Questo documento descrive come modificare i diversi cifrari usati da ISE 3.3 e versioni successive in diversi servizi in modo che gli utenti abbiano il controllo su tali meccanismi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componente utilizzato

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Suite di crittografia supportate

Cisco ISE supporta TLS versioni 1.0, 1.1 e 1.2.

Da Cisco ISE release 3.3, TLS 1.3 è stato introdotto solo per l'interfaccia grafica Admin. Queste cifrature sono supportate per l'accesso HTTPS di amministrazione su TL 1.3 :

- TLS_AES_128_GCM_SHA256

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE supporta i certificati server RSA ed ECDSA. Sono supportate le seguenti curve ellittiche:

- secp256r1
- secp384r1
- secp521r1

Nella tabella seguente vengono elencate le suite di cifratura supportate:

Cipher Suite	Autenticazione EAP/DTLS RADIUS	Download CRL da HTTPS o comunicazione Secure LDAP/Secure Syslog/DTLS CoA
ECDHE-ECDSA-AES256-GCM-SHA384	Sì, quando è consentito TLS 1.1.	Sì, quando è consentito TLS 1.1.
ECDHE-ECDSA-AES128-GCM-SHA256	Sì, quando è consentito TLS 1.1.	Sì, quando è consentito TLS 1.1.
ECDHE-ECDSA-AES256-SHA384	Sì, quando è consentito TLS 1.1.	Sì, quando è consentito TLS 1.1.
ECDHE-ECDSA-AES128-SHA256	Sì, quando è consentito TLS 1.1.	Sì, quando è consentito TLS 1.1.
ECDHE-ECDSA-AES256-SHA	Sì, quando è consentito SHA-1.	Sì, quando è consentito SHA-1.
ECDHE-ECDSA-AES128-SHA	Sì, quando è consentito SHA-1.	Sì, quando è consentito SHA-1.
ECDHE-RSA-AES256-GCM-SHA384	Sì, quando è consentito l'ECDHE-RSA.	Sì quando è consentito l'ECDHE-RSA.
ECDHE-RSA-AES128-GCM-SHA256	Sì, quando è consentito l'ECDHE-RSA.	Sì, quando è consentito l'ECDHE-RSA.

ECDHE-RSA-AES256-SHA384	Sì, quando è consentito l'ECDHE-RSA.	Sì, quando è consentito l'ECDHE-RSA.
ECDHE-RSA-AES128-SHA256	Sì, quando è consentito l'ECDHE-RSA.	Sì, quando è consentito l'ECDHE-RSA.
ECDHE-RSA-AES256-SHA	Sì, quando è consentito ECDHE-RSA/SHA-1.	Sì, quando è consentito ECDHE-RSA/SHA-1.
ECDHE-RSA-AES128-SHA	Sì, quando è consentito ECDHE-RSA/SHA-1.	Sì, quando è consentito ECDHE-RSA/SHA-1.
DHE-RSA-AES256-SHA256	No	Sì
DHE-RSA-AES128-SHA256	No	Sì
DHE-RSA-AES256-SHA	No	Sì, quando è consentito SHA-1.
DHE-RSA-AES128-SHA	No	Sì, quando è consentito SHA-1.
AES256-SHA256	Sì	Sì
AES128-SHA256	Sì	Sì
AES256-SHA	Sì, quando è consentito SHA-1.	Sì, quando è consentito SHA-1.
AES128-SHA	Sì, quando è consentito SHA-1.	Sì, quando è consentito SHA-1.
DES-CBC3-SHA	Sì, quando è consentito 3DES/SHA-1.	Sì, quando è consentito 3DES/SHA-1.
DHE-DSS-AES256-SHA	No	Sì, quando 3DES/DSS e SHA-1 sono abilitati.
DHE-DSS-AES128-SHA	No	Sì, quando 3DES/DSS e SHA-1

		sono abilitati.
EDH-DSS-DES-CBC3-SHA	No	Sì, quando 3DES/DSS e SHA-1 sono abilitati.
RC4-SHA	Quando l'opzione Consenti cifratura debole è abilitata nella pagina Protocolli consentiti e quando è consentito SHA-1.	No
RC4-MD5	Quando l'opzione Consenti cifratura debole è abilitata nella pagina Protocolli consentiti e quando è consentito SHA-1.	No
Solo provisioning anonimo AP-FAST: ADH-AES-128-SHA	Sì	No
Convalida utilizzo chiavi	Il certificato client può avere KeyUsage=Key Agreement e ExtendedKeyUsage=Client Authentication per queste cifrature: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Convalida ExtendedKeyUsage	Il certificato client deve avere KeyUsage=Key Encipherment e ExtendedKeyUsage=Autenticazione client per queste cifrature: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA	Il certificato del server deve avere ExtendedKeyUsage=Autenticazione server.

	• DHE-RSA-AES128-SHA	

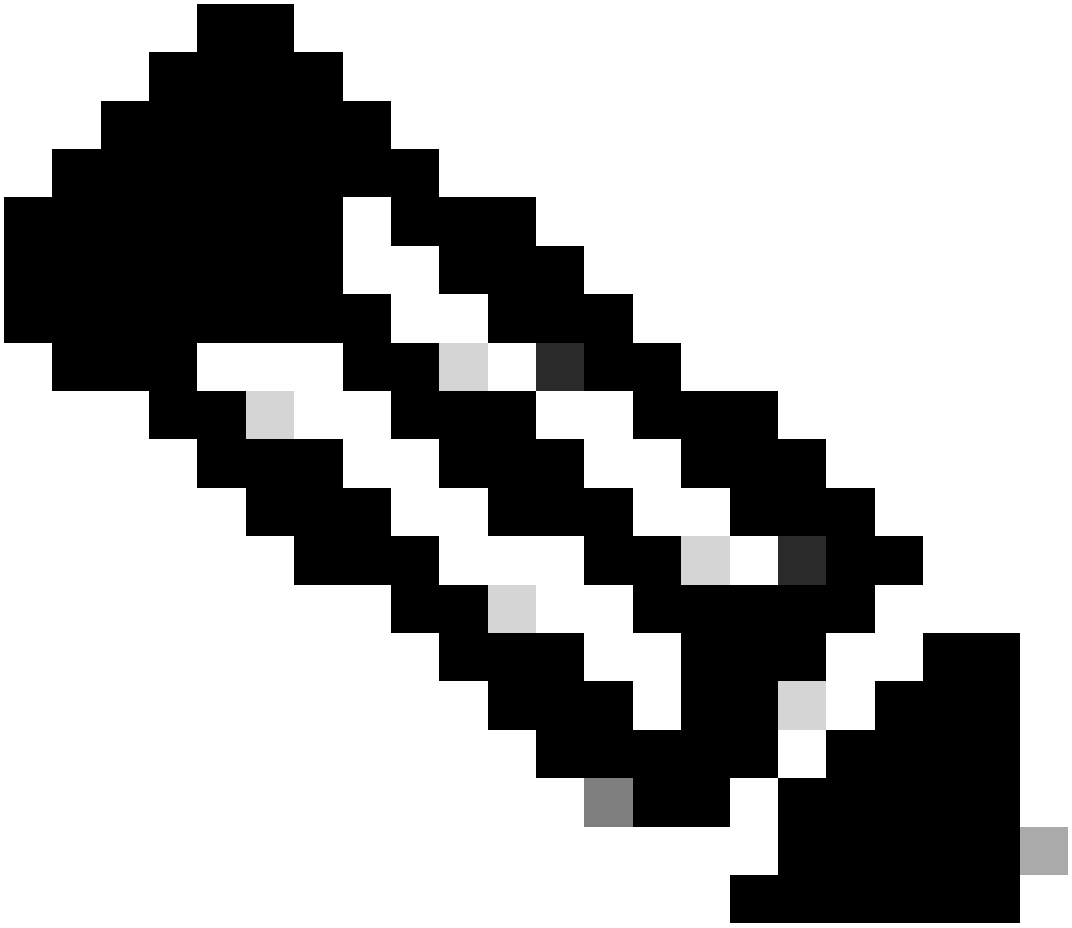
Configurazioni

Configura impostazioni di protezione

Per configurare le impostazioni di protezione, eseguire la procedura seguente:

1. Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu ( ) e scegliere Amministrazione > Sistema > Impostazioni > Impostazioni protezione.

2. Nella sezione Impostazioni versioni TLS, scegliere una o un intervallo di versioni TLS consecutive. Selezionare la casella di controllo accanto alle versioni TLS che si desidera abilitare.



Nota: TLS 1.2 è abilitato per impostazione predefinita e non può essere disabilitato. Se si scelgono più versioni TLS, è necessario scegliere versioni consecutive. Ad esempio, se si sceglie TLS 1.0, TLS 1.1 viene attivato automaticamente. Cambiando le cifrature in questa posizione si potrebbe riavviare ISE.

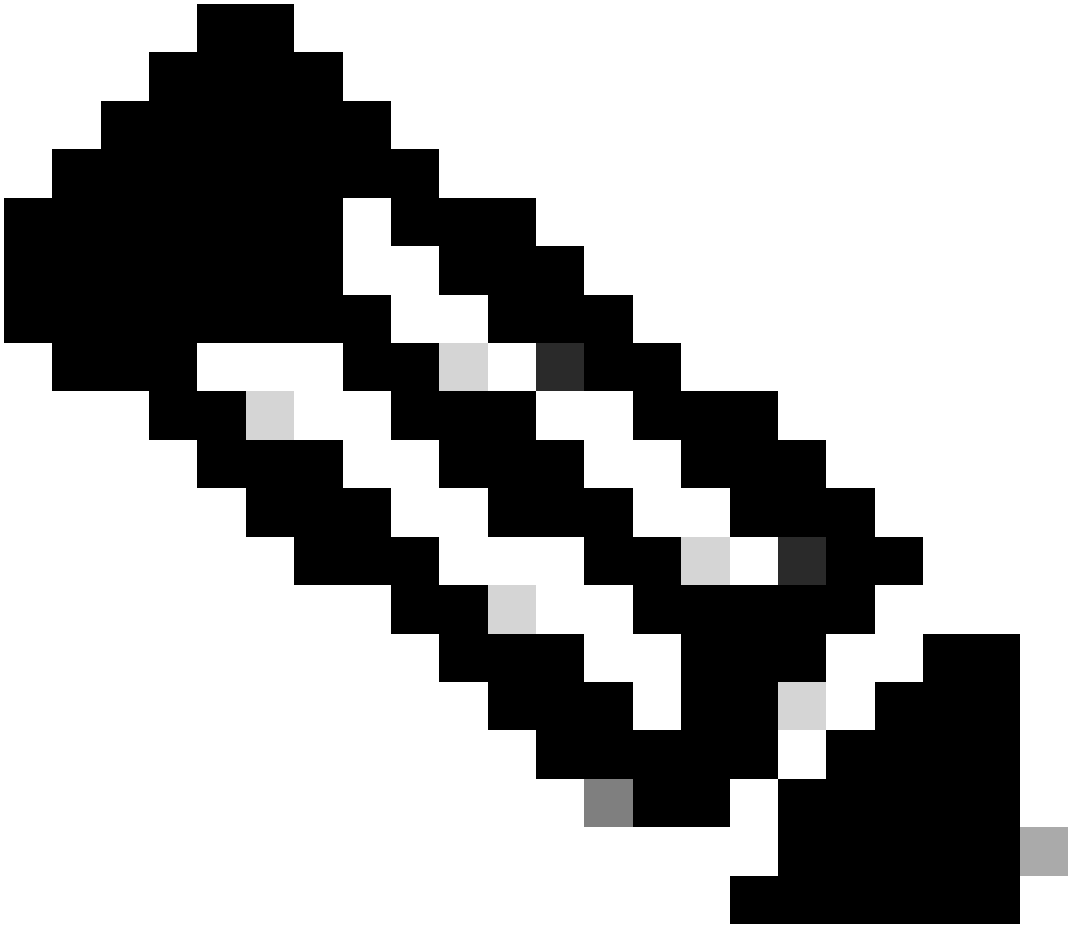
Consenti TLS 1.0, 1.1 e 1.2: abilita TLS 1.0, 1.1 e 1.2 per i servizi successivi. Inoltre, consenti cifratura SHA-1: consente ai cifrari SHA-1 di comunicare con i peer per questi flussi di lavoro:

- Autenticazione EAP
- Download CRL dal server HTTPS.
- Comunicazione syslog sicura tra ISE e il server syslog esterno.
- ISE come client LDAP sicuro.
- ISE è un client ODBC sicuro.
- Servizi ERS.
- servizi pxGrid.
- Tutti i portali ISE (ad esempio, il portale per i guest, il portale per il provisioning dei client e il portale MyDevices).

- Comunicazione MDM.
- Comunicazione agente ID passivo.
- Provisioning dell'Autorità di certificazione.
- Accesso all'interfaccia utente dell'amministratore.

Queste porte vengono utilizzate dai componenti elencati in alto per la comunicazione:

- Accesso amministratore: 443
- Cisco ISE Portals: 9002, 8443, 8444, 8445, 8449 o qualsiasi porta configurata per i portali ISE.
- ERS: 9060, 9061, 9063
- pxGrid: 8.910



Nota: l'opzione Consenti cifratura SHA-1 è disabilitata per default. Per una maggiore sicurezza, si consiglia di utilizzare i cifrari SHA-256 o SHA-384.

È necessario riavviare tutti i nodi in una distribuzione dopo aver abilitato o disabilitato l'opzione Consenti cifratura SHA-1. Se il riavvio non riesce, le modifiche alla configurazione non vengono applicate.

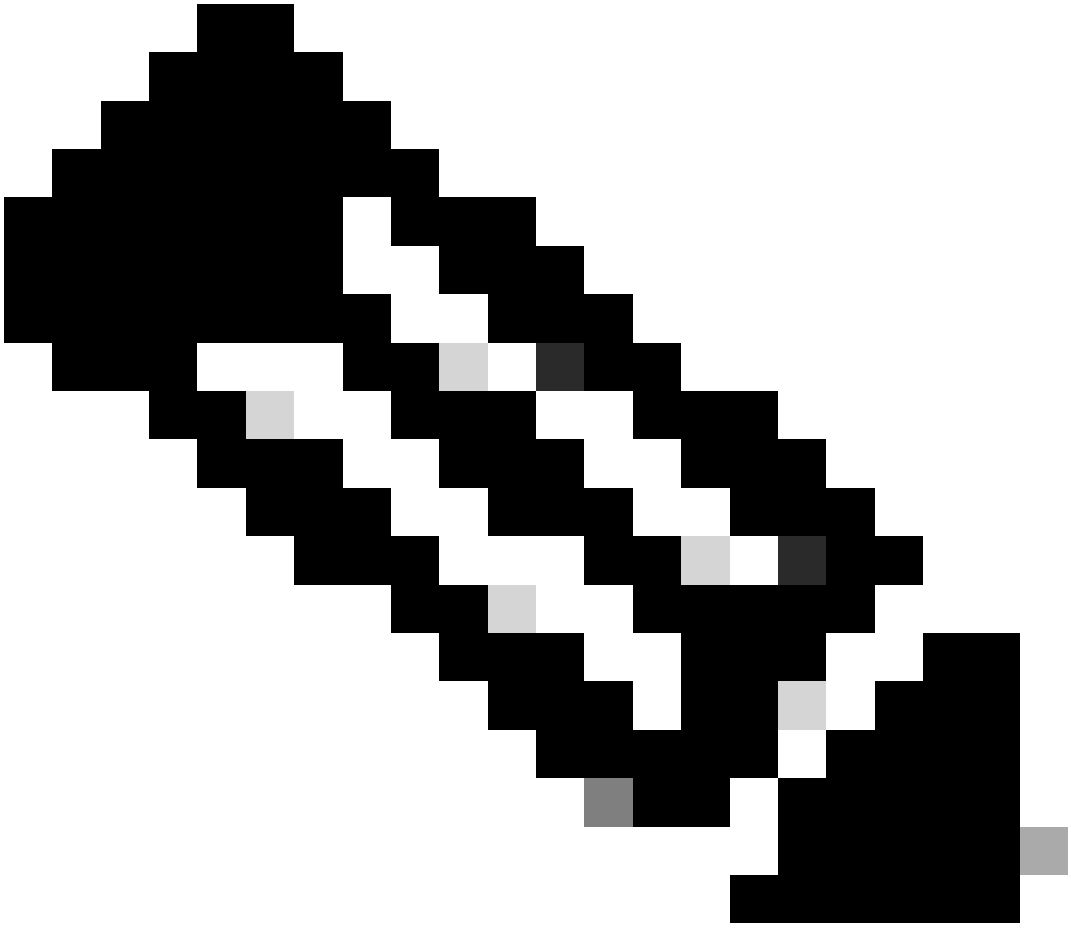
Quando l'opzione Allow SHA-1 Ciphers è disabilitata, se un client con solo cifratura SHA-1 tenta di connettersi a Cisco ISE, l'handshake ha esito negativo ed è possibile visualizzare un messaggio di errore nel browser del client.

Scegliere una delle opzioni consentendo ai cifrari SHA-1 di comunicare con i peer legacy:

- Consenti tutte le cifrature SHA-1: consente a tutte le cifrature SHA-1 di comunicare con i peer legacy.
- Consenti solo TLS_RSA_WITH_AES_128_CBC_SHA: consente solo la cifratura TLS_RSA_WITH_AES_128_CBC_SHA di comunicare con i peer legacy.

Consenti TLS 1.3: consente a TLS 1.3 l'accesso HTTPS dell'amministratore sulla porta 443 per:

- Cisco ISE Admin GUI
- API abilitate per la porta 443 (Open API, ERS, MnT).



Nota: le comunicazioni AAA e tutti i tipi di comunicazioni tra nodi non supportano TLS 1.3. Abilitare TLS 1.3 su Cisco ISE e sui client e server rilevanti per l'accesso amministrativo su TLS 1.3.

Consenti cifratura ECDHE-RSA e 3DES: consente la comunicazione tra cifratura ECDHE-RSA e peer per questi flussi di lavoro:

- Cisco ISE è configurato come server EAP
- Cisco ISE è configurato come server DTLS RADIUS
- Cisco ISE è configurato come client DTLS RADIUS
- Cisco ISE scarica CRL da HTTPS o da un server LDAP sicuro
- Cisco ISE è configurato come client syslog sicuro
- Cisco ISE è configurato come client LDAP sicuro

Consenti cifrature DSS per ISE come client: quando Cisco ISE opera come client, consente alle cifrature DSS di comunicare con un server per questi flussi di lavoro:

- Cisco ISE è configurato come client DTLS RADIUS
- Cisco ISE scarica CRL da HTTPS o da un server LDAP sicuro
- Cisco ISE è configurato come client syslog sicuro
- Cisco ISE è configurato come client LDAP sicuro

Consenti rinegoziazione TLS unsafe legacy per ISE come client: consente la comunicazione con i server TLS legacy che non supportano la rinegoziazione TLS sicura per questi flussi di lavoro:

- Cisco ISE scarica CRL da HTTPS o da un server LDAP sicuro
- Cisco ISE è configurato come client syslog sicuro
- Cisco ISE è configurato come client LDAP sicuro

Divulgazione nomi utente non validi: per impostazione predefinita, Cisco ISE visualizza il messaggio non valido per errori di autenticazione a causa di nomi utente non corretti. Per facilitare il debug, questa opzione forza Cisco ISE a visualizzare i nomi utente nei report, anziché il messaggio non valido. Si noti che i nomi utente vengono sempre visualizzati per le autenticazioni non riuscite non dovute a nomi utente non corretti.

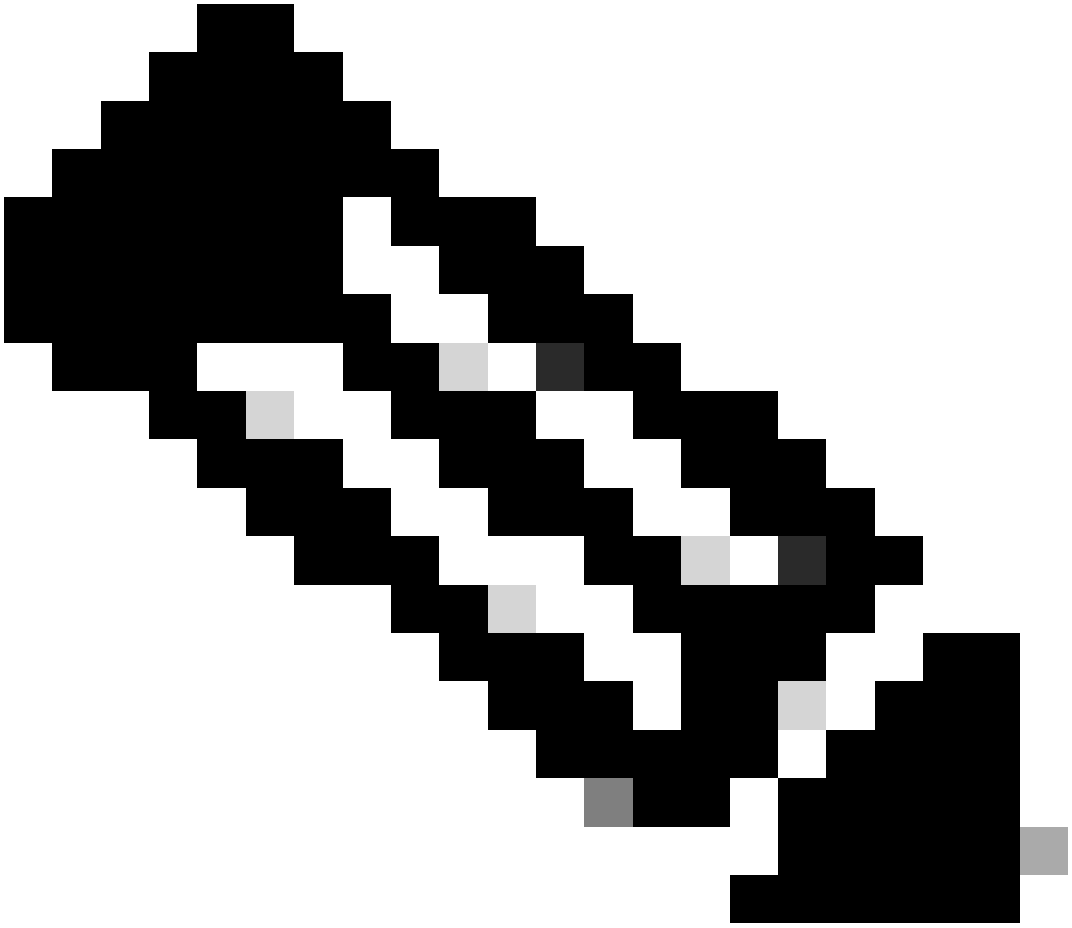
Questa funzionalità è supportata per le origini di identità Active Directory, Internal Users, LDAP e ODBC. Non è supportato per altre origini di identità, ad esempio token RADIUS, RSA o SAML.

Usa certificati basati su FQDN per le comunicazioni con fornitori di terze parti (TC-NAC): i certificati basati su FQDN devono essere conformi alle seguenti regole:

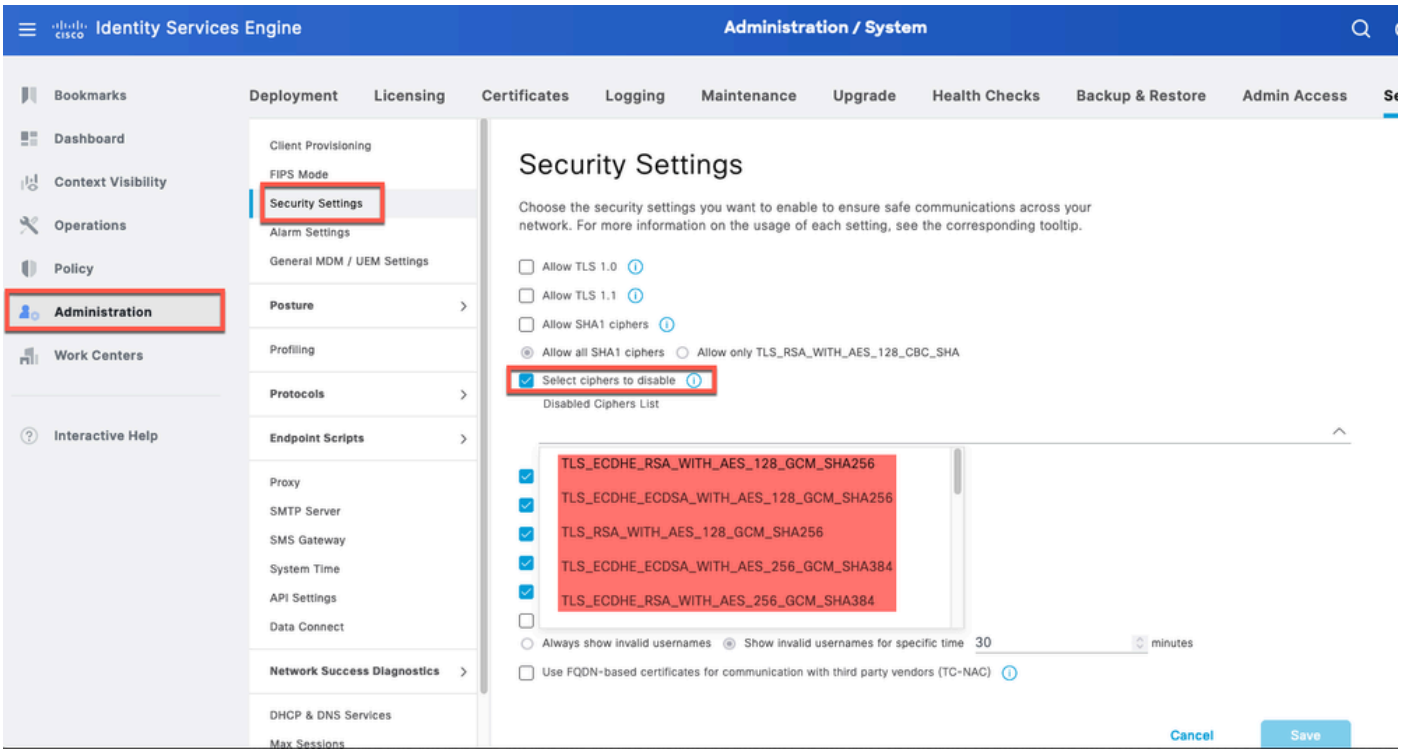
- I campi SAN e CN nel certificato devono contenere valori FQDN. Nomi host e indirizzi IP non supportati.
- I certificati con caratteri jolly devono contenere il carattere jolly solo nel frammento all'estrema sinistra.
- L'FQDN specificato in un certificato deve essere risolvibile tramite DNS.

Disabilita crittografia specifica

Selezionare l'opzione Configura manualmente elenco cifrari per configurare manualmente i cifrari in modo che comunichino con questi componenti di Cisco ISE: admin UI, ERS, OpenAPI, secure ODBC, portals e pxGrid. Viene visualizzato un elenco di cifrari con i cifrari consentiti già selezionati. Ad esempio, se l'opzione Consenti cifratura SHA1 è attivata, i cifrari SHA1 saranno attivati in questo elenco. Se l'opzione Consenti solo TLS_RSA_WITH_AES_128_CBC_SHA è selezionata, in questo elenco viene abilitata solo questa cifratura SHA1. Se l'opzione Consenti cifratura SHA1 è disattivata, non è possibile attivare alcuna cifratura SHA1 in questo



Nota: quando si modifica l'elenco di cifrari da disabilitare, l'application server viene riavviato su tutti i nodi Cisco ISE. Quando la modalità FIPS è attivata o disattivata, gli application server su tutti i nodi vengono riavviati, con un conseguente downtime significativo del sistema. Se sono stati disattivati dei cifrari mediante l'opzione Configura manualmente elenco cifrari, controllare l'elenco dei cifrari disattivati dopo il riavvio degli application server. L'elenco dei cifrari disattivati non è stato modificato a causa della transizione alla modalità FIPS.



Opzione per disabilitare Ciphers ISE 3.3

- Dalla CLI di ISE è possibile eseguire il comando application configure isee usare l'opzione 37, evidenziata in questa schermata, **Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS**. Il bug correlato è l'ID bug Cisco CSCwb77915.

```
isedemo-33/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
```

Opzione per disabilitare/abilitare RSA_PSS per EAP-TLS

Informazioni correlate

-

Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).