ISE 3.3 이상에서 암호 구성

목차

소개

이 문서에서는 사용자가 이러한 메커니즘을 제어할 수 있도록 ISE 3.3 이상에서 다른 서비스에서 사용하는 서로 다른 암호를 수정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용된 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.3.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

지원되는 암호 그룹

Cisco ISE는 TLS 버전 1.0, 1.1 및 1.2를 지원합니다.

Cisco ISE 릴리스 3.3에서는 TLS 1.3이 관리 GUI용으로만 도입되었습니다. 이러한 암호는 TL 1.3을 통한 관리자 HTTPS 액세스에 지원됩니다.

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE는 RSA 및 ECDSA 서버 인증서를 지원 합니다. 다음과 같은 타원 커브가 지원됩니다.

- secp256r1
- secp384r1
- 섹션p521r1

이 표에는 지원되는 암호 그룹이 나열되어 있습니다.

암호 그룹	EAP 인증/RADIUS DTLS	HTTPS 또는 보안 LDAP/보안 Syslog 통신/DTLS CoA에서 CRL 다운로드
ECDHE-ECDSA-AES256-GCM-SHA384	예, TLS 1.1이 허용되는 경우.	예, TLS 1.1이 허용되는 경우.
ECDHE-ECDSA-AES128-GCM-SHA256	예, TLS 1.1이 허용되는 경우.	예, TLS 1.1이 허용되는 경우.
ECDHE-ECDSA-AES256-SHA384	예, TLS 1.1이 허용되는 경우.	예, TLS 1.1이 허용되는 경우.
ECDHE-ECDSA-AES128-SHA256	예, TLS 1.1이 허용되는 경우.	예, TLS 1.1이 허용되는 경우.
ECDHE-ECDSA-AES256-SHA	예, SHA-1이 허용되는 경우.	예, SHA-1이 허용되는 경우.
ECDHE-ECDSA-AES128-SHA	예, SHA-1이 허용되는 경우.	예, SHA-1이 허용되는 경우.
ECDHE-RSA-AES256-GCM-SHA384	예, ECDHE-RSA가 허용되는 경우.	예, ECDHE-RSA가 허용되는 경우.
ECDHE-RSA-AES128-GCM-SHA256	예, ECDHE-RSA가 허용되는 경우.	예, ECDHE-RSA가 허용되는 경우.
ECDHE-RSA-AES256-SHA384	예, ECDHE-RSA가 허용되는 경우.	예, ECDHE-RSA가 허용되는 경우.
ECDHE-RSA-AES128-SHA256	예, ECDHE-RSA가 허용되는 경우.	예, ECDHE-RSA가 허용되는 경우.

ECDHE-RSA-AES256-SHA	예, ECDHE-RSA/SHA-1이 허용되는 경우.	예, ECDHE-RSA/SHA-1이 허용되는 경우.
ECDHE-RSA-AES128-SHA	예, ECDHE-RSA/SHA-1이 허용되는 경우.	예, ECDHE-RSA/SHA-1이 허용되는 경우.
DHE-RSA-AES256-SHA256	아니요	예
DHE-RSA-AES128-SHA256	아니요	예
DHE-RSA-AES256-SHA	아니요	예, SHA-1이 허용되는 경우.
DHE-RSA-AES128-SHA	아니요	예, SHA-1이 허용되는 경우.
AES256-SHA256	예	예
AES128-SHA256	예	예
AES256-SHA	예, SHA-1이 허용되는 경우.	예, SHA-1이 허용되는 경우.
AES128-SHA	예, SHA-1이 허용되는 경우.	예, SHA-1이 허용되는 경우.
DES-CBC3-SHA	예, 3DES/SHA-1이 허용되는 경우.	예, 3DES/SHA-1이 허용되는 경우.
DHE-DSS-AES256-SHA	아니요	예, 3DES/DSS 및 SHA-1이 활성화된 경우.
DHE-DSS-AES128-SHA	아니요	예, 3DES/DSS 및 SHA-1이 활성화된 경우.
EDH-DSS-DES-CBC3-SHA	아니요	예, 3DES/DSS 및 SHA-1이 활성화된 경우.
RC4-SHA	Allowed Protocols 페이지에서 Allow weak ciphers 옵션이 활성화되고 SHA-1이 허용되는 경우.	아니요

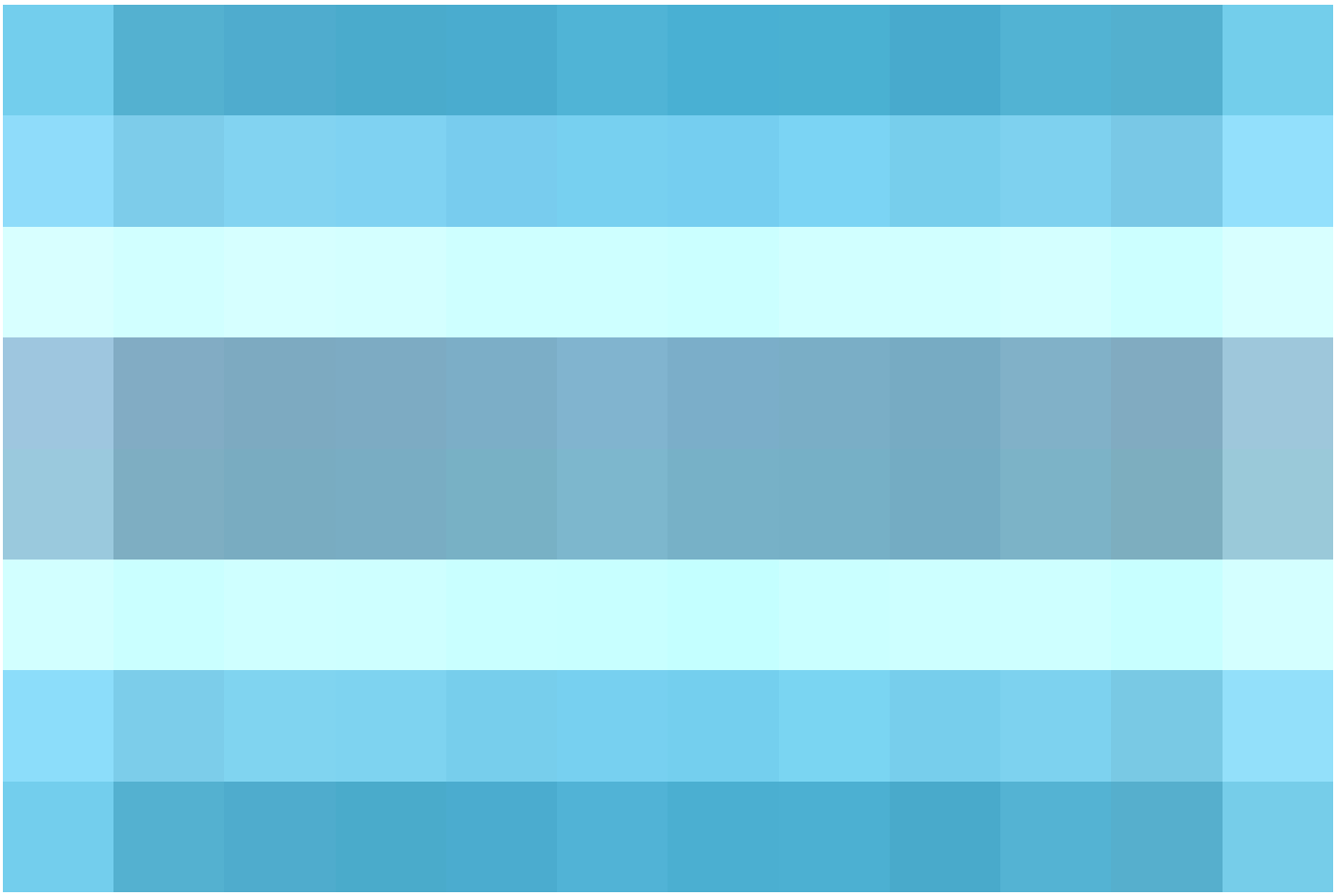
RC4-MD5	Allowed Protocols 페이지에서 Allow weak ciphers 옵션이 활성화되고 SHA-1이 허용되는 경우.	아니요
AP-FAST 익명 프로비저닝 전용: ADH-AES-128-SHA	예	아니요
KeyUsage 검증	클라이언트 인증서에는 다음 암호에 대한 KeyUsage=Key Agreement 및 ExtendedKeyUsage=Client Authentication이 있을 수 있습니다. • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
ExtendedKeyUsage 확인	클라이언트 인증서에는 다음 암호에 대한 KeyUsage=Key Encipherment 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다. • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	서버 인증서에는 ExtendedKeyUsage=Server Authentication이 있어야 합니다.

설정

보안 설정 구성

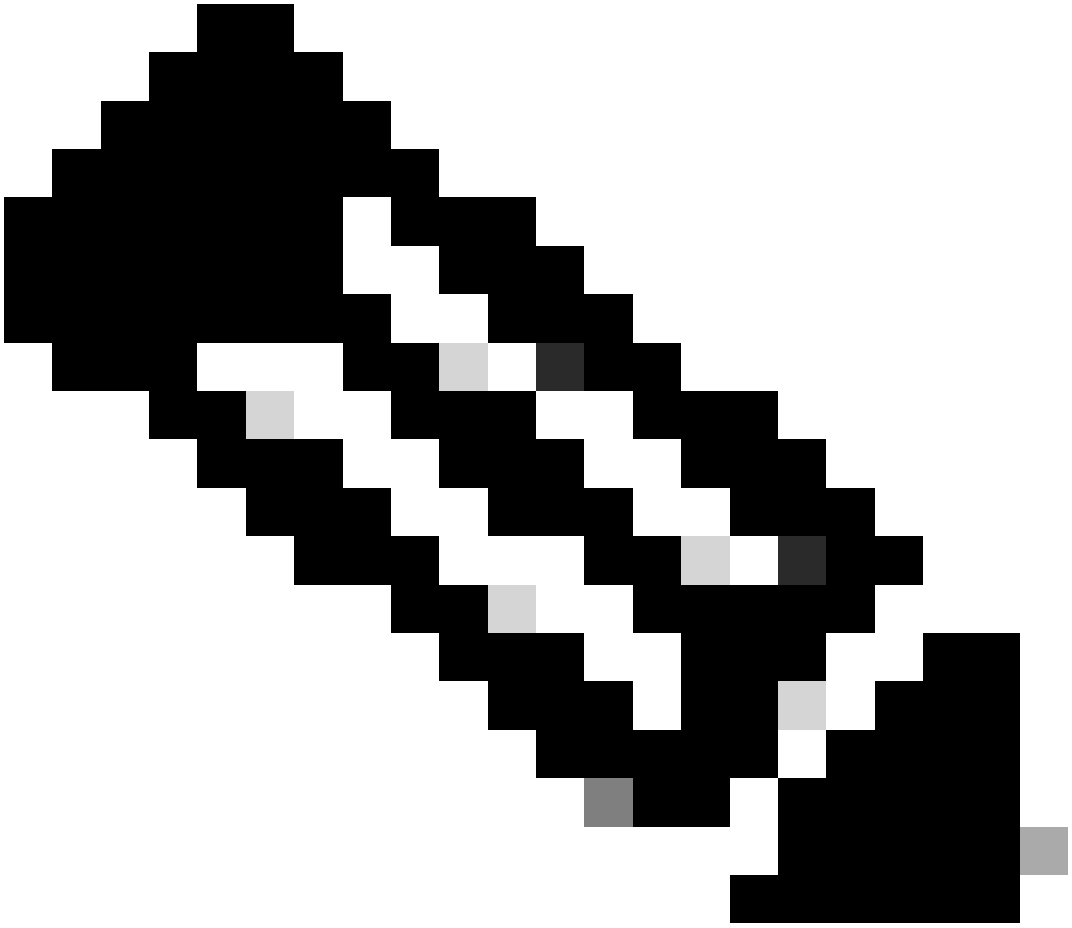
보안 설정을 구성하려면 다음 절차를 수행합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(



)을 클릭하고 Administration(관리) > System(시스템) > Settings(설정) > Security Settings(보안 설정)를 선택합니다.

2. TLS Versions Settings(TLS 버전 설정) 섹션에서 하나 이상의 연속 TLS 버전을 선택합니다. 활성화할 TLS 버전 옆의 확인란을 선택합니다.



참고: TLS 1.2는 기본적으로 활성화되어 있으며 비활성화할 수 없습니다. 둘 이상의 TLS 버전을 선택하는 경우 연속 버전을 선택해야 합니다. 예를 들어, TLS 1.0을 선택하면 TLS 1.1이 자동으로 활성화됩니다. 여기서 암호를 변경하면 ISE가 다시 시작될 수 있습니다.

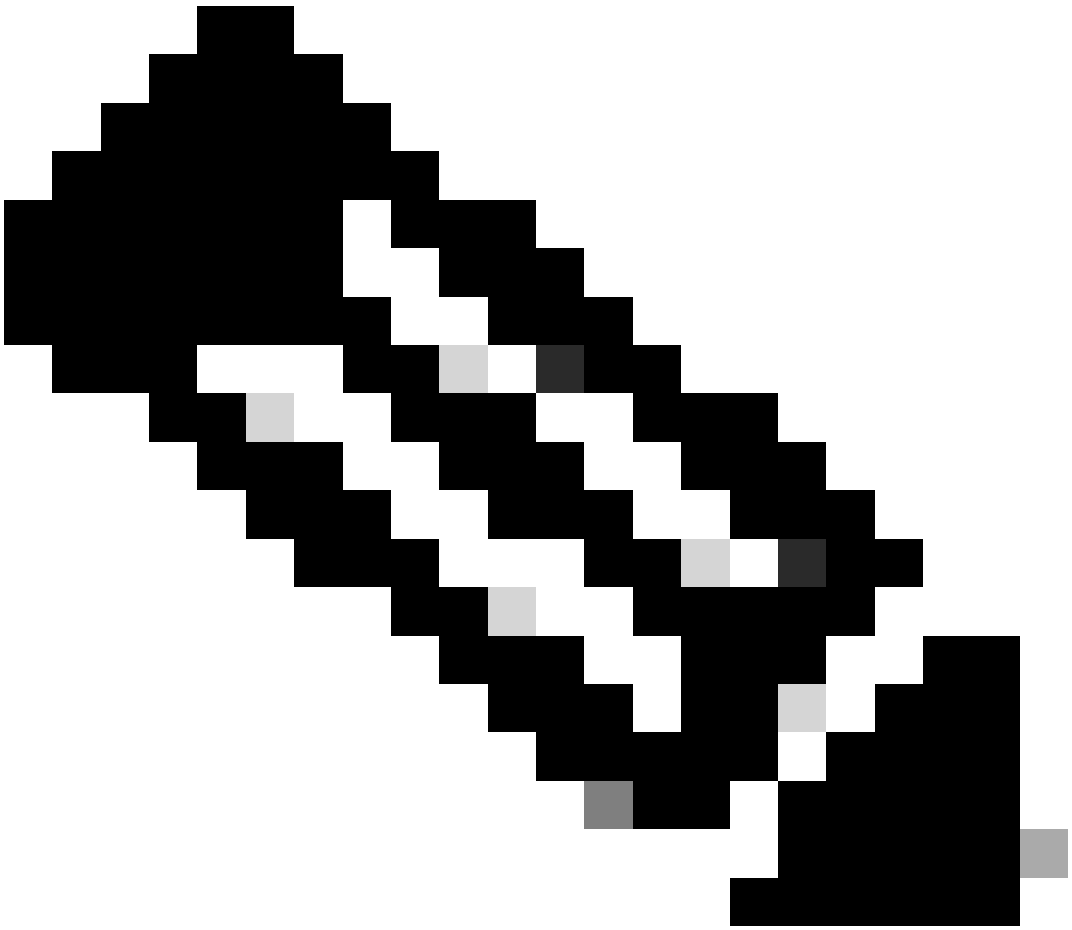
Allow TLS 1.0, 1.1 and 1.2(TLS 1.0, 1.1 및 1.2 허용): 다음 서비스에 TLS 1.0, 1.1 및 1.2를 활성화합니다. 또한 SHA-1 암호 허용: SHA-1 암호가 다음 워크플로에 대해 피어와 통신할 수 있도록 허용합니다.

- EAP 인증.
- HTTPS 서버에서 CRL 다운로드.
- ISE와 외부 syslog 서버 간의 보안 Syslog 통신
- ISE를 보안 LDAP 클라이언트로 사용
- ISE를 보안 ODBC 클라이언트로 사용
- ERS 서비스
- pxGrid 서비스.
- 모든 ISE 포털(예: 게스트 포털, 클라이언트 프로비저닝 포털, 내 디바이스 포털).
- MDM 커뮤니케이션.

- PassiveID 에이전트 통신
- Certificate Authority 프로비저닝
- 관리자 GUI 액세스.

이러한 포트는 통신을 위해 위에 나열된 구성 요소에서 사용됩니다.

- 관리자 액세스: 443
- Cisco ISE 포털: 9002, 8443, 8444, 8445, 8449 또는 ISE 포털에 대해 구성된 모든 포트.
- ERS: 9060, 9061, 9063
- pxGrid: 8910



참고: Allow SHA-1 Ciphers(SHA-1 암호 허용) 옵션은 기본적으로 비활성화되어 있습니다. 보안을 강화하려면 SHA-256 또는 SHA-384 암호를 사용하는 것이 좋습니다.

Allow SHA-1 Ciphers(SHA-1 암호 허용) 옵션을 활성화하거나 비활성화한 후 구축의 모든 노드를

다시 시작해야 합니다. 재시작에 성공하지 못하면 컨피그레이션 변경 사항이 적용되지 않습니다.

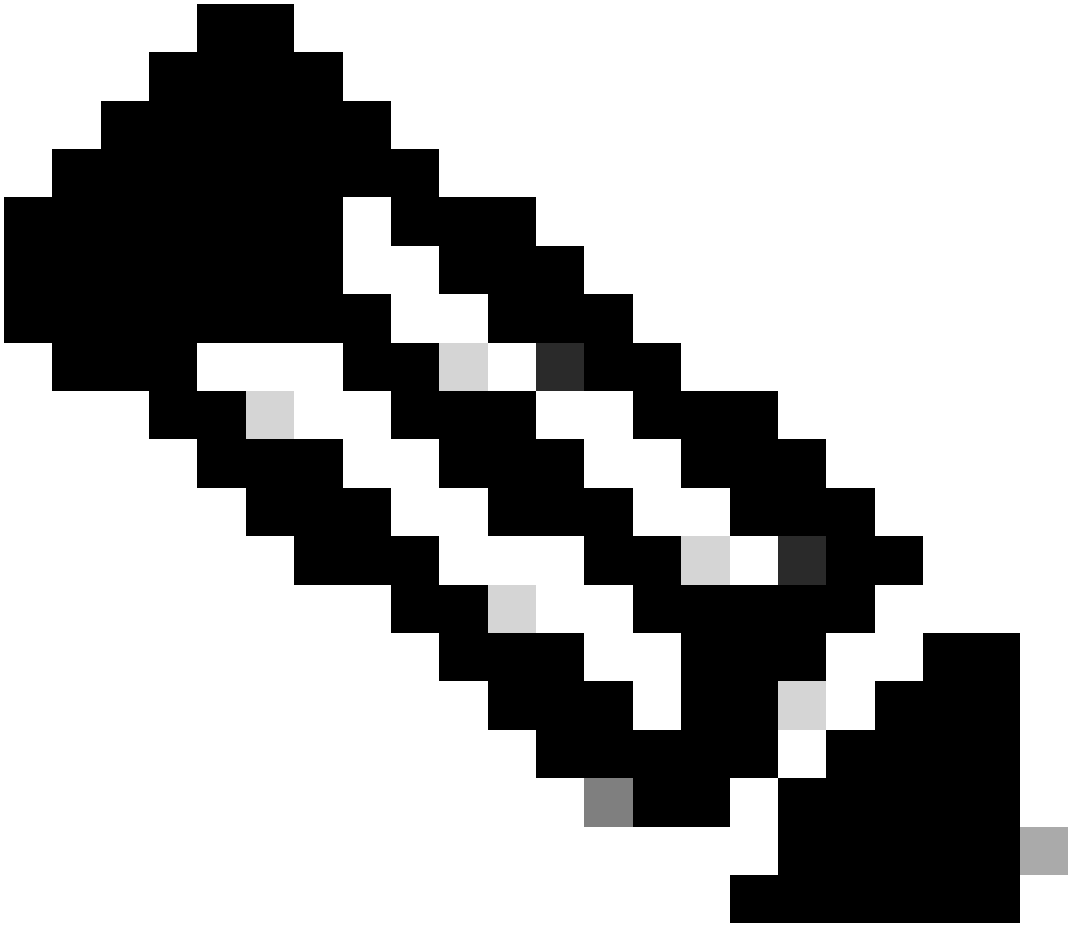
Allow SHA-1 Ciphers(SHA-1 암호 허용) 옵션이 비활성화된 경우 SHA-1 암호만 있는 클라이언트가 Cisco ISE에 연결하려고 하면 핸드셰이크가 실패하고 클라이언트 브라우저에 오류 메시지가 표시될 수 있습니다.

SHA-1 암호가 레거시 피어와 통신할 수 있도록 허용하는 동안 옵션 중 하나를 선택합니다.

- Allow all SHA-1 Ciphers(모든 SHA-1 암호 허용): 모든 SHA-1 암호가 레거시 피어와 통신할 수 있도록 허용합니다.
- TLS_RSA_WITH_AES_128_CBC_SHA만 허용: TLS_RSA_WITH_AES_128_CBC_SHA 암호만 레거시 피어와의 통신을 허용합니다.

Allow TLS 1.3(TLS 1.3 허용): 다음에 대해 포트 443을 통한 관리자 HTTPS 액세스를 위한 TLS 1.3을 허용합니다.

- Cisco ISE 관리 GUI
- 포트 443에 대해 활성화된 API(Open API, ERS, MnT).



참고: AAA 통신 및 모든 유형의 노드 간 통신은 TLS 1.3을 지원하지 않습니다. Cisco ISE에서 TLS 1.3을 활성화하고 TLS 1.3을 통한 관리자 액세스를 위해 관련 클라이언트 및 서버를 활성화합니다.

Allow ECDHE-RSA and 3DES Ciphers(ECDHE-RSA 및 3DES 암호 허용): ECDHE-RSA 암호가 다음 워크플로에 대해 피어와 통신할 수 있도록 허용합니다.

- Cisco ISE는 EAP 서버로 구성 됩니다
- Cisco ISE는 RADIUS DTLS 서버로 구성 되어 있습니다
- Cisco ISE는 RADIUS DTLS 클라이언트로 구성 되어 있습니다
- Cisco ISE는 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드 합니다
- Cisco ISE는 보안 syslog 클라이언트로 구성 됩니다
- Cisco ISE는 보안 LDAP 클라이언트로 구성 됩니다

클라이언트로 ISE에 대한 DSS 암호 허용: Cisco ISE가 클라이언트로 작동할 때 DSS 암호는 다음과 같은 워크플로를 위해 서버와 통신할 수 있습니다.

- Cisco ISE는 RADIUS DTLS 클라이언트로 구성 되어 있습니다
- Cisco ISE는 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드 합니다
- Cisco ISE는 보안 syslog 클라이언트로 구성 됩니다
- Cisco ISE는 보안 LDAP 클라이언트로 구성 됩니다

Allow Legacy Unsafe TLS Renegotiation for ISE as a Client(클라이언트로 ISE에 대해 레거시 안전하지 않은 TLS 재협상 허용): 다음 워크플로에 대해 안전한 TLS 재협상을 지원하지 않는 레거시 TLS 서버와의 통신을 허용합니다.

- Cisco ISE는 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드 합니다
- Cisco ISE는 보안 syslog 클라이언트로 구성 됩니다
- Cisco ISE는 보안 LDAP 클라이언트로 구성 됩니다

잘못된 사용자 이름 공개: 기본적으로 Cisco ISE는 잘못된 사용자 이름으로 인한 인증 실패에 대해 잘못된 메시지를 표시합니다. 디버깅을 지원하기 위해 이 옵션은 Cisco ISE가 잘못된 메시지 대신 보고서에 사용자 이름을 표시하도록 합니다. 사용자 이름이 잘못되어 있지 않은 인증에 실패한 경우 항상 사용자 이름이 표시됩니다.

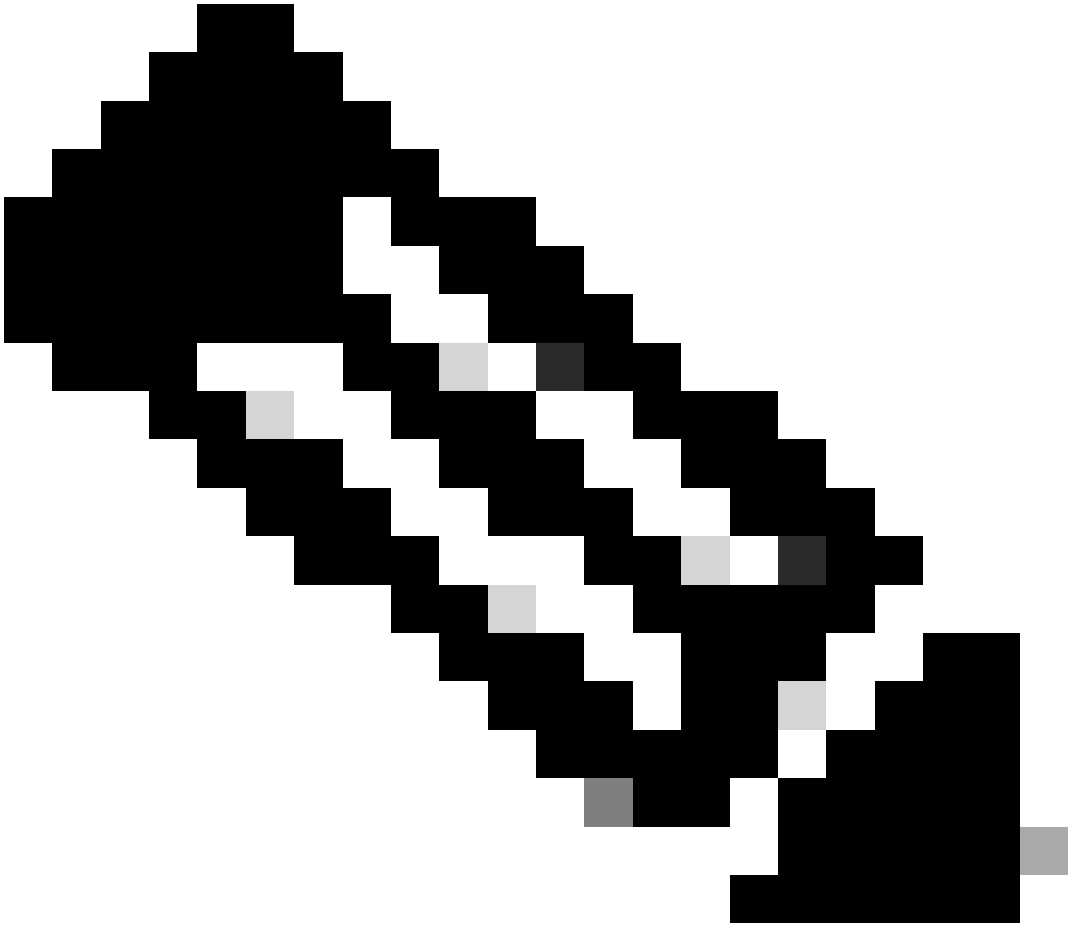
이 기능은 Active Directory, 내부 사용자, LDAP 및 ODBC ID 소스에 대해 지원됩니다. RADIUS 토큰, RSA 또는 SAML과 같은 다른 ID 소스에 대해서는 지원되지 않습니다.

서드파티 벤더(TC-NAC)와의 통신에 FQDN 기반 인증서 사용: FQDN 기반 인증서는 다음 규칙을 준수해야 합니다.

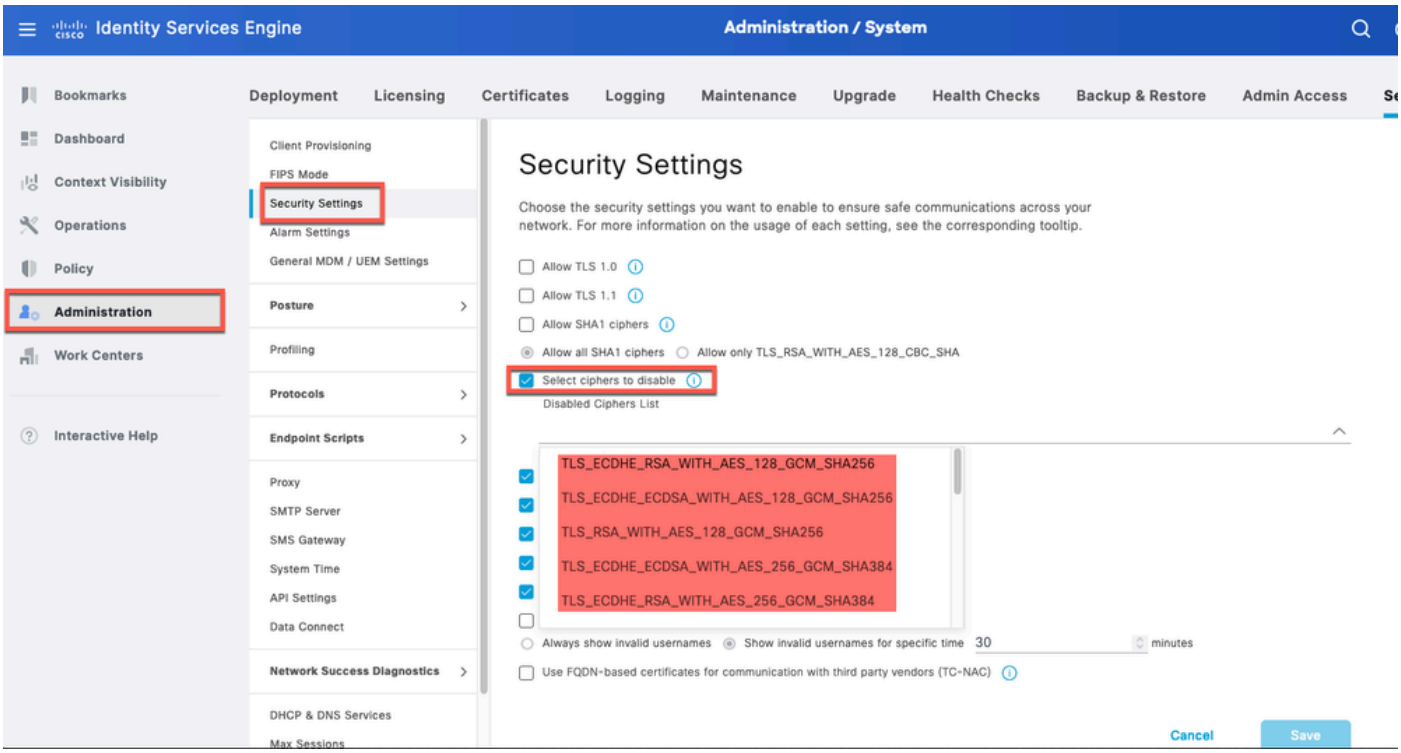
- 인증서의 SAN 및 CN 필드는 FQDN 값을 포함해야 합니다. 호스트 이름 및 IP 주소는 지원되지 않습니다.
- 와일드카드 인증서는 맨 왼쪽 조각에만 와일드카드 문자를 포함해야 합니다.
- 인증서에 제공된 FQDN은 DNS를 확인할 수 있어야 합니다.

특정 암호 사용 안 함

admin UI, ERS, OpenAPI, secure ODBC, portals, pxGrid와 같은 Cisco ISE 구성 요소와 통신하도록 암호를 수동으로 구성하려면 Manually Configure Ciphers List(암호 목록 수동 구성) 옵션을 선택합니다. 이미 선택된 허용 암호와 함께 암호 목록이 표시됩니다. 예를 들어, Allow SHA1 Ciphers(SHA1 암호 허용) 옵션이 활성화된 경우 이 목록에서 SHA1 암호가 활성화됩니다. Allow Only TLS_RSA_WITH_AES_128_CBC_SHA(TLS_RSA_WITH_CBC_SHA만 허용) 옵션이 선택된 경우 이 목록에서 이 SHA1 암호만 활성화됩니다. Allow SHA1 Ciphers(SHA1 암호 허용) 옵션이 비활성화된 경우 이 옵션에서 SHA1 암호를 활성화할 수 없습니다



참고: 비활성화할 암호 목록을 수정하면 모든 Cisco ISE 노드에서 애플리케이션 서버가 다시 시작됩니다. FIPS 모드가 활성화 또는 비활성화되면 모든 노드의 애플리케이션 서버가 다시 시작되어 시스템 다운타임이 크게 발생합니다. Manually Configure Ciphers List 옵션을 사용하여 암호를 비활성화한 경우 애플리케이션 서버를 다시 시작한 후 비활성화된 암호 목록을 확인합니다. 비활성화된 암호 목록은 FIPS 모드 전환 때문에 변경되지 않습니다.



암호화 ISE 3.3을 비활성화하는 옵션

- ISE CLI에서 명령을 실행하고 이 스크린샷에서 강조 표시된 옵션 37인 EAP-TLS용 RSA_PSS 서명의 Enable/Disable/Current_status를 사용할 수 application configure ise있습니다. 관련 버그는 Cisco 버그 ID CSCwb77915입니다.

```
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
```

EAP-TLS용 RSA_PSS 비활성화/활성화 옵션

관련 정보

-

Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.