

# ISE 3.3以降での暗号の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[サポートされる暗号スイート](#)

---

## はじめに

このドキュメントでは、ユーザがこのようなメカニズムを制御できるように、ISE 3.3以降で使用されるさまざまな暗号を異なるサービスで変更する方法について説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.3.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## サポートされる暗号スイート

Cisco ISEはTLSバージョン1.0、1.1、および1.2をサポートします。

Cisco ISEリリース3.3以降、TLS 1.3は管理GUI専用として導入されました。次の暗号は、TL 1.3経由の管理HTTPSアクセスでサポートされています。

- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256

Cisco ISEは、RSAおよびECDSAサーバ証明書をサポートします。次の楕円曲線がサポートされています。

- secp256r1
- secp384r1
- secp521r1

次の表に、サポートされている暗号スイートを示します。

Cipher Suite	EAP認証/RADIUS DTLS	HTTPSまたはセキュアLDAP/セキュアSyslog通信/DTLS CoAからのCRLのダウンロード
ECDHE-ECDSA-AES256-GCM-SHA384	はい。TLS 1.1が許可されている場合。	はい。TLS 1.1が許可されている場合。
ECDHE-ECDSA-AES128-GCM-SHA256	はい。TLS 1.1が許可されている場合。	はい。TLS 1.1が許可されている場合。
ECDHE-ECDSA-AES256-SHA384	はい。TLS 1.1が許可されている場合。	はい。TLS 1.1が許可されている場合。
ECDHE-ECDSA-AES128-SHA256	はい。TLS 1.1が許可されている場合。	はい。TLS 1.1が許可されている場合。
ECDHE-ECDSA-AES256-SHA	はい。SHA-1が許可される場合。	はい。SHA-1が許可される場合。
ECDHE-ECDSA-AES128-SHA	はい。SHA-1が許可される場合。	はい。SHA-1が許可される場合。
ECDHE-RSA-AES256-GCM-SHA384	はい。ECDHE-RSAが許可されている場合。	はい ( ECDHE-RSAが許可されている場合 )
ECDHE-RSA-AES128-GCM-SHA256	はい。ECDHE-RSAが許可されている場合。	はい。ECDHE-RSAが許可されている場合。
ECDHE-RSA-AES256-SHA384	はい。ECDHE-RSAが許可されている場合。	はい。ECDHE-RSAが許可されている場合。

ECDHE-RSA-AES128-SHA256	はい。ECDHE-RSAが許可されている場合。	はい。ECDHE-RSAが許可されている場合。
ECDHE-RSA-AES256-SHA	はい。ECDHE-RSA/SHA-1が許可されている場合。	はい。ECDHE-RSA/SHA-1が許可されている場合。
ECDHE-RSA-AES128-SHA	はい。ECDHE-RSA/SHA-1が許可されている場合。	はい。ECDHE-RSA/SHA-1が許可されている場合。
DHE-RSA-AES256-SHA256	いいえ	Yes
DHE-RSA-AES128-SHA256	いいえ	Yes
DHE-RSA-AES256-SHA	いいえ	はい。SHA-1が許可される場合。
DHE-RSA-AES128-SHA	いいえ	はい。SHA-1が許可される場合。
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	はい。SHA-1が許可される場合。	はい。SHA-1が許可される場合。
AES128-SHA	はい。SHA-1が許可される場合。	はい。SHA-1が許可される場合。
DES-CBC3-SHA	はい。3DES/SHA-1が許可されている場合。	はい。3DES/SHA-1が許可されている場合。
DHE-DSS-AES256-SHA	いいえ	はい。3DES/DSSおよびSHA-1が有効な場合にサポートされます。
DHE-DSS-AES128-SHA	いいえ	はい。3DES/DSSおよびSHA-1が有効な場合にサポートされ

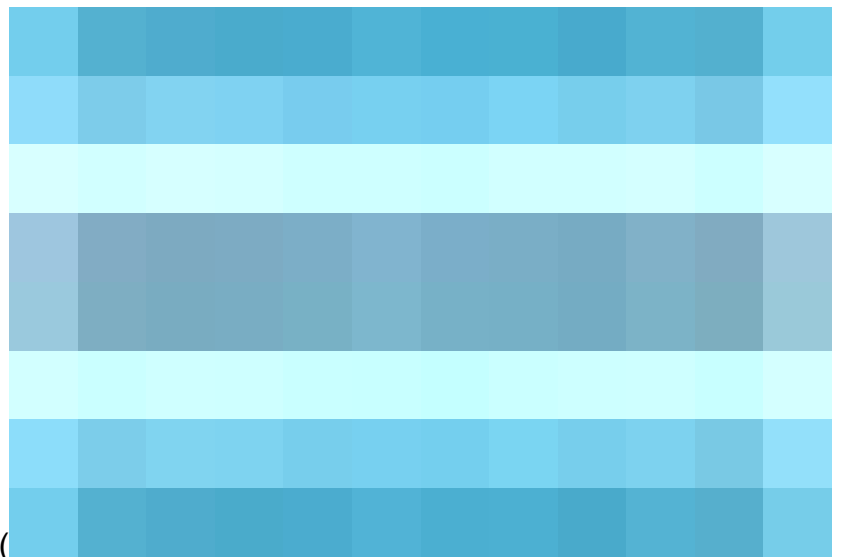
		ます。
EDH-DSS-DES-CBC3-SHA	いいえ	はい。3DES/DSSおよびSHA-1が有効な場合にサポートされます。
RC4-SHA	Allowed Protocolsページで Allow weak ciphersオプションがイネーブルになっている場合、およびSHA-1が許可されている場合。	いいえ
RC4-MD5	Allowed Protocolsページで Allow weak ciphersオプションがイネーブルになっている場合、およびSHA-1が許可されている場合。	いいえ
AP-FAST匿名プロビジョニングのみ : ADH-AES-128-SHA	Yes	いいえ
KeyUsageの検証	<p>クライアント証明書には、次の暗号に対するKeyUsage=Key Agreementおよび ExtendedKeyUsage=Client Authenticationを指定できます。</p> <ul style="list-style-type: none"> <li>• ECDHE-ECDSA-AES128-GCM-SHA256</li> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• ECDHE-ECDSA-AES128-SHA256</li> <li>• ECDHE-ECDSA-AES256-SHA384</li> </ul>	
ExtendedKeyUsageの検証	<p>クライアント証明書には、次の暗号に対するKeyUsage=Key Enciphermentおよび ExtendedKeyUsage=Client Authenticationが必要です。</p>	<p>サーバー証明書には ExtendedKeyUsage=Server Authenticationが必要です。</p>

	<ul style="list-style-type: none"><li>• AES256-SHA256</li><li>• AES128-SHA256</li><li>• AES256-SHA</li><li>• AES128-SHA</li><li>• DHE-RSA-AES128-SHA</li></ul>	
--	--	--

## コンフィギュレーション

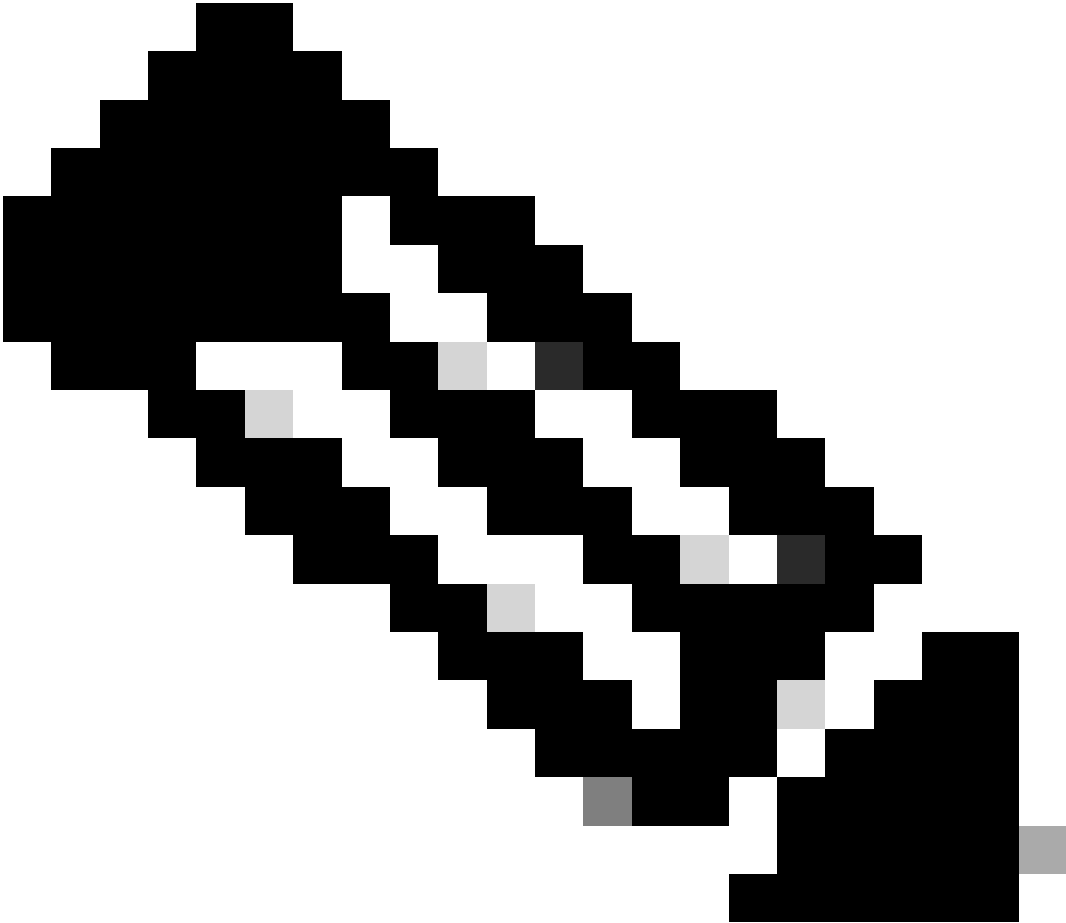
### セキュリティ設定の構成

セキュリティ設定を行うには、次の手順を実行します。



1. Cisco ISE GUIで、メニューアイコン( )をクリックし、Administration > System > Settings > Security Settingsの順に選択します。
2. 「TLSバージョン設定」セクションで、連続するTLSバージョンを1つまたは複数選択します。有効にするTLSバージョンの横にあるチェックボックスをオンにします。

---



注:TLS 1.2はデフォルトで有効になっており、無効にすることはできません。複数のTLSバージョンを選択する場合は、連続するバージョンを選択する必要があります。たとえば、TLS 1.0を選択すると、TLS 1.1が自動的に有効になります。ここで暗号を変更すると、ISEが再起動する可能性があります。

---

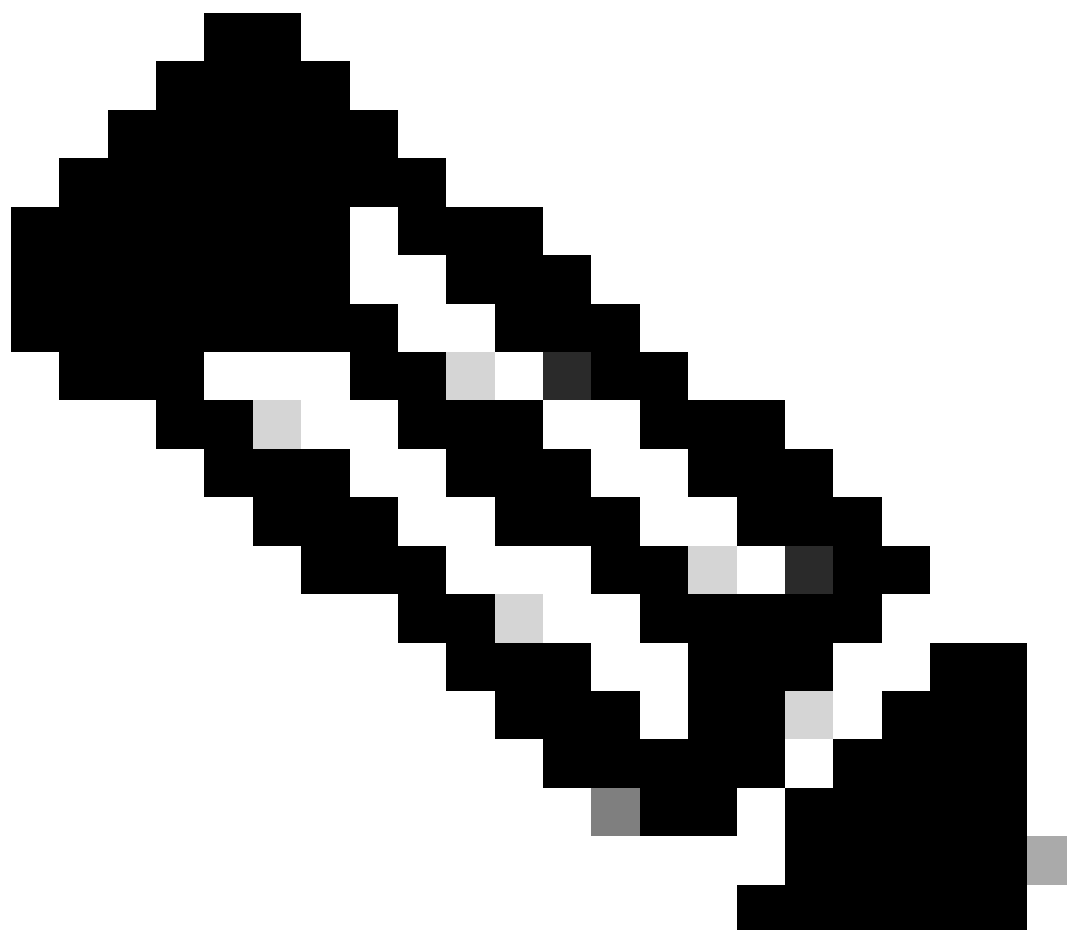
Allow TLS 1.0, 1.1 and 1.2 : 次のサービスに対してTLS 1.0, 1.1 and 1.2を有効にします。また、SHA-1暗号を許可 : 次のワークフローでSHA-1暗号がピアと通信できるようにします。

- EAP Authentication.
- HTTPSサーバからのCRLダウンロード
- ISEと外部syslogサーバ間のSyslog通信を保護します。
- セキュアLDAPクライアントとしてのISE。
- セキュアなODBCクライアントとしてのISE。
- ERSサービス。
- pxGridサービス。
- すべてのISEポータル ( ゲストポータル、クライアントプロビジョニングポータル、マイデバイスポータルなど )

- MDM通信。
- PassiveIDエージェント通信。
- 認証局のプロビジョニング
- 管理GUIアクセス。

上にリストされているコンポーネントでは、次のポートが通信に使用されます。

- 管理者アクセス : 443
- Cisco ISEポータル : 9002、8443、8444、8445、8449、またはISEポータル用に設定された任意のポート。
- ERS: 9060、9061、9063
- pxGrid:8910



注 : デフォルトでは、Allow SHA-1 Ciphersオプションは無効になっています。セキュリティを強化するために、SHA-256またはSHA-384暗号を使用することをお勧めします。

---

Allow SHA-1 Ciphersオプションを有効または無効にした後は、導入のすべてのノードを再起動する必要があります。再起動に失敗した場合、設定変更は適用されません。

Allow SHA-1 Ciphersオプションが無効になっている場合、SHA-1暗号のみを使用するクライアントがCisco ISEに接続しようとする、ハンドシェイクが失敗し、クライアントブラウザにエラーメッセージが表示されます。

SHA-1暗号がレガシーピアと通信できるようにしながら、次のいずれかのオプションを選択します。

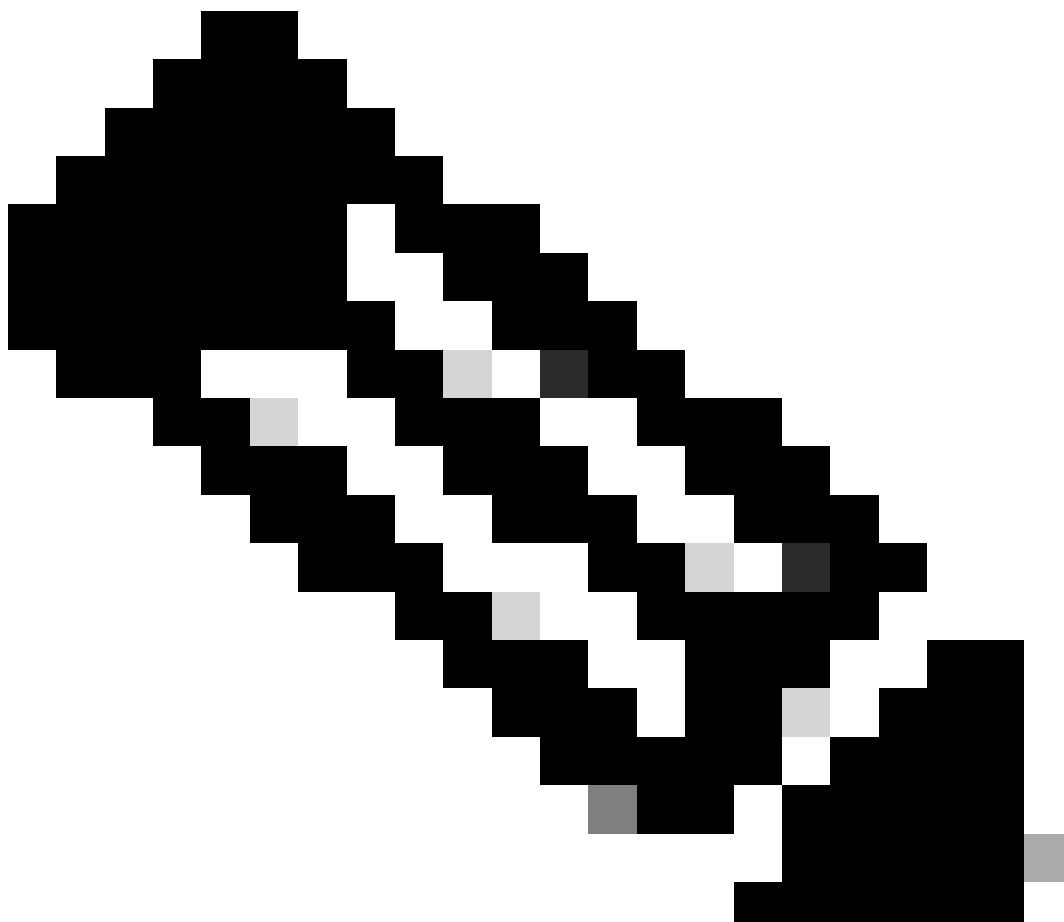
- すべてのSHA-1暗号を許可する：すべてのSHA-1暗号がレガシーピアと通信できるようにします。
- Allow only TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA:TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA暗号のみを使用して、レガシーピアと通信できます。

Allow TLS 1.3：管理者がポート443経由でTLS 1.3にHTTPSアクセスすることを許可します。

- Cisco ISE管理GUI
- ポート443(Open API、ERS、MnT)に対して有効なAPI



---



注:AAA通信およびすべてのタイプのノード間通信は、TLS 1.3をサポートしていません。  
Cisco ISEおよび関連するクライアントとサーバで、TLS 1.3を介した管理者アクセス用に  
TLS 1.3を有効にします。

---

Allow ECDHE-RSA and 3DES Ciphers : 次のワークフローで、ECDHE-RSA暗号がピアと通信できるようにします。

- Cisco ISEがEAPサーバとして設定されている
- Cisco ISEがRADIUS DTLSサーバとして設定されている
- Cisco ISEがRADIUS DTLSクライアントとして設定されている
- Cisco ISEがHTTPSまたはセキュアLDAPサーバからCRLをダウンロードする
- Cisco ISEは、セキュアなsyslogクライアントとして設定されます
- Cisco ISEがセキュアLDAPクライアントとして設定されている

クライアントとしてISEのDSS暗号を許可する: Cisco ISEがクライアントとして動作する場合、DSS暗号は次のワークフローでサーバと通信できます。

- Cisco ISEがRADIUS DTLSクライアントとして設定されている
- Cisco ISEがHTTPSまたはセキュアLDAPサーバからCRLをダウンロードする
- Cisco ISEは、セキュアなsyslogクライアントとして設定されます
- Cisco ISEがセキュアLDAPクライアントとして設定されている

Allow Legacy Unsafe TLS Renegotiation for ISE as a Client : 次のワークフローに対する安全なTLS再ネゴシエーションをサポートしていないレガシーTLSサーバとの通信を許可します。

- Cisco ISEがHTTPSまたはセキュアLDAPサーバからCRLをダウンロードする
- Cisco ISEは、セキュアなsyslogクライアントとして設定されます
- Cisco ISEがセキュアLDAPクライアントとして設定されている

無効なユーザ名の開示 : デフォルトでは、ユーザ名が誤っているために認証が失敗すると、Cisco ISEに無効なメッセージが表示されます。デバッグに役立つように、このオプションは、無効なメッセージの代わりに、レポートにユーザ名を表示するようにCisco ISEに強制します。ユーザ名が正しくないために失敗した認証に対しては、ユーザ名が常に表示されることに注意してください。

この機能は、Active Directory、内部ユーザ、LDAP、およびODBCの各アイデンティティ・ソースでサポートされています。RADIUSトークン、RSA、SAMLなどの他のアイデンティティ・ソースではサポートされていません。

サードパーティベンダー(TC-NAC)との通信にFQDNベースの証明書を使用する:FQDNベースの証明書は、次のルールに準拠する必要があります。

- 証明書のSANフィールドとCNフィールドには、FQDN値が含まれている必要があります。ホスト名とIPアドレスはサポートされていません。
- ワイルドカード証明書には、ワイルドカード文字を一番左のフラグメントにのみ含める必要があります。
- 証明書で提供されるFQDNは、DNSで解決できる必要があります。

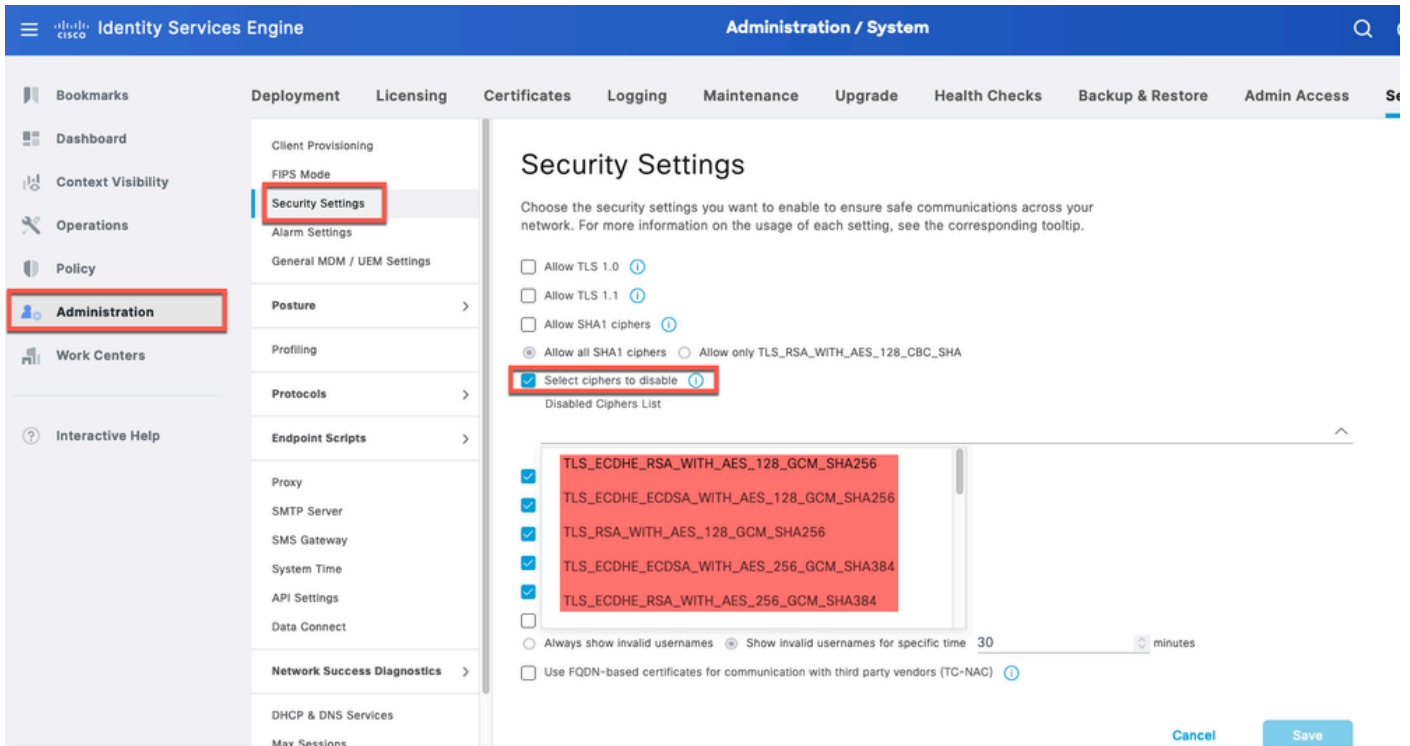
## 特定の暗号を無効にする

admin UI、ERS、OpenAPI、セキュアODBC、ポータル、およびpxGridの各Cisco ISEコンポーネントと通信するように暗号を手動で設定する場合は、暗号リストの手動設定オプションをオンにします。許可されている暗号がすでに選択された状態で、暗号のリストが表示されます。たとえば、Allow SHA1 Ciphersオプションが有効になっている場合、このリストではSHA1暗号が有効になります。Allow Only TLS\_RSA\_WITH\_AES\_128\_CBC\_SHAオプションを選択すると、このSHA1暗号だけがこのリストで有効になります。Allow SHA1 Ciphersオプションがディセーブルの場合、この設定でSHA1暗号を



注：無効にする暗号のリストを編集すると、アプリケーションサーバがすべてのCisco ISEノードで再起動します。FIPSモードを有効または無効にすると、すべてのノードのアプリケーションサーバが再起動され、システムのダウンタイムが大幅に増加します。Manually Configure Ciphers Listオプションを使用して暗号を無効にしている場合は、アプリケーションサーバの再起動後に、無効になっている暗号のリストを確認してください。FIPSモードの移行のため、無効な暗号のリストは変更されません。

---



暗号を無効にするオプションISE 3.3

- ISE CLIからコマンド `application configure ise` を実行し、オプション37 (このスクリーンショットで強調表示) を使用できます。EAP-TLS用のRSA\_PSSシグニチャのEnable/Disable/Current\_status。関連するバグは、Cisco Bug ID [CSCwb77915](https://bugzilla.cisco.com/show_bug.cgi?id=CSCwb77915) です。

```

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 REPLUGINS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
LOJEXT

```

EAP-TLSに対してRSA\_PSSを無効/有効にするオプション

関連情報

- 

[シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。