

ISEでの証明書更新の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ISE 自己署名証明書の表示](#)

[証明書を変更する時期の特定](#)

[証明書署名要求の生成](#)

[証明書のインストール](#)

[警告システムの設定](#)

[確認](#)

[警告システムの確認](#)

[証明書変更の確認](#)

[証明書の確認](#)

[トラブルシューティング](#)

[結論](#)

概要

このドキュメントでは、Cisco Identity Services Engine (ISE) で証明書を更新するためのベストプラクティスとプロアクティブな手順について説明します。また、証明書の期限切れなどの差し迫ったイベントについて管理者に警告できるように、アラームと通知を設定する方法についても説明します。

注：このドキュメントは、証明書の診断ガイドではありません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- X509 証明書
- Cisco ISE と証明書の設定

使用するコンポーネント

"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、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、コマンドの潜在的な影響について確実に理解しておく必要があります」

- Cisco ISE リリース 3.0.0.458
- アプライアンスまたは VMware

背景説明

ISE 管理者は、いずれは ISE 証明書が期限切れになる状況を経験します。ISE サーバに期限切れの証明書がある場合、期限切れの証明書を新しい有効な証明書で置き換えない限り、深刻な問題が発生する可能性があります。

注：拡張認証プロトコル(EAP)に使用される証明書の有効期限が切れると、クライアントが ISE 証明書を信頼しなくなるため、すべての認証が失敗する可能性があります。ISE 管理証明書が期限切れになると、リスクはさらに大きくなります。管理者は ISE にログインできなくなり、分散導入は機能を停止して複製を行えなくなります。

ISE 管理者は、古い証明書が期限切れになる前に、新しい有効な証明書を ISE にインストールする必要があります。このプロアクティブなアプローチにより、ダウンタイムを防止または最小限に抑え、エンドユーザーへの影響を回避できます。新しくインストールされた証明書の期間が始まると、新しい証明書で EAP/Admin またはその他の役割を有効にできます。

古い証明書が期限切れになる前にアラームを発生させ、新しい証明書のインストールを管理者に通知するように ISE を設定できます。

注：このドキュメントでは、証明書の更新の影響を実証するために、自己署名証明書として ISE 管理証明書を使用しますが、この方法は実稼働システムには推奨されません。EAP ロールと管理者ロールの両方に CA 証明書を使用することをお勧めします。

設定

ISE 自己署名証明書の表示

ISE をインストールすると、自己署名証明書が生成されます。自己署名証明書は、管理アクセス、分散型展開内の通信 (HTTPS)、およびユーザー認証 (EAP) に使用されます。実稼働システムでは、自己署名証明書ではなく CA 証明書を使用してください。

ヒント：追加情報については、『[Cisco Identity Services Engine Hardware Installation Guide, Release 3.0](#)』の「[Certificate Management in Cisco ISE](#)」の項を参照してください

[9](#)

ISE 証明書の形式は、プライバシー強化メール (PEM) または Distinguished Encoding Rules (DER) にする必要があります。

最初の自己署名証明書を表示するには、図のように、ISE GUI で [Administration] > [System] > [Certificates] > [System Certificates] に移動します。

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Certificate Management									
System Certificates									
Trusted Certificates									
OCSP Client Profile									
Certificate Signing Requests									
Certificate Periodic Check Se...									
Certificate Authority									
abtomar31									
<input type="checkbox"/>	OU=ISE Messaging Service,CN=abtomar31.abtomar.local	ISE Messaging Service		abtomar31.abtomar.local	Certificate Services Endpoint Sub CA - abtomar31	Mon, 3 May 2021	Mon, 4 May 2026	●	
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=abtomar31.abtomar.local	pxGrid		abtomar31.abtomar.local	Certificate Services Endpoint Sub CA - abtomar31	Mon, 3 May 2021	Mon, 4 May 2026	●	
<input type="checkbox"/>	Default self-signed server certificate - CN=SAML_abtomar31.abtomar.local	SAML		SAML_abtomar31.abtomar.local	SAML_abtomar31.abtomar.local	Tue, 4 May 2021	Sun, 3 May 2026	●	
<input type="checkbox"/>	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Thu, 4 May 2023	●	

証明書署名要求 (CSR) を介して ISE にサーバー証明書をインストールし、Admin または EAP プロトコルに関して証明書を変更しても、自己署名サーバー証明書は残りますが、未使用のステータスになります。

注意： Admin プロトコルの変更の場合は、ISE サービスの再起動が必要です。これにより、数分のダウンタイムが発生します。EAP プロトコルの変更は、ISE サービスの再起動がトリガーされず、ダウンタイムが発生しません。

証明書を変更する時期の特定

インストールされた証明書がもうすぐ期限切れになるとします。証明書が期限切れになってから更新するのと、証明書が期限切れになる前に変更するのとどちらが適切だと思いますか。証明書の切り替えを計画し、切り替えによって発生するダウンタイムを管理する時間を確保するには、有効期限が切れる前に証明書を変更する必要があります。

証明書はいつ変更する必要がありますか。開始日が古い証明書の失効日より前である新しい証明書を取得します。この2つの日付の間の期間が移行期間です。

注意： Admin を有効にすると、ISE サーバーでサービスが再起動し、数分間のダウンタイムが発生します。

次の図は、間もなく期限切れになる証明書の情報を示しています。

<input type="checkbox"/>	Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Wed, 5 May 2021	▼
--------------------------	--	--	----------------------------------	-------------------------	-------------------------	-----------------	-----------------	---

証明書署名要求の生成

次の手順では、CSR を介して証明書を更新する方法を説明します。

1. ISE コンソールで [Administration] > [System] > [Certificates] > [Certificate Signing Requests] に移動して、[Generate Certificate Signing Request] をクリックします。

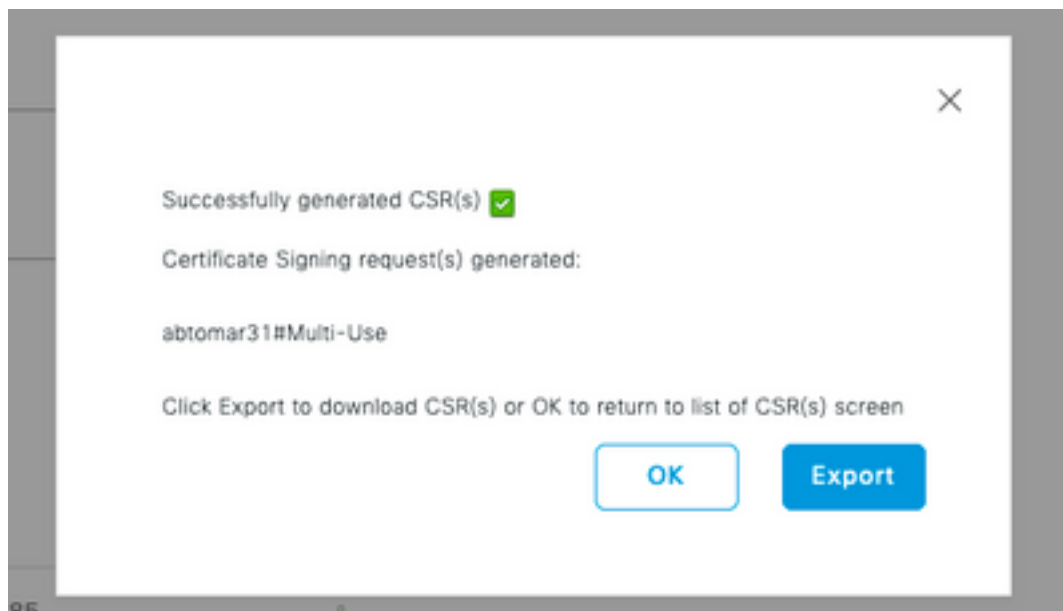
2. [Certificate Subject] テキスト フィールドに入力する必要がある最小限の情報は CN=ISEfqdn です。ここで、ISEfqdn は ISE の完全修飾ドメイン名 (FQDN) です。O (組織)、OU (組織単位)、C (国) などのフィールドをカンマで区切って [Certificate Subject] に追加します。

The screenshot shows the Cisco ISE Administration interface for the 'Certificates' section. The 'Subject' field is highlighted with a red box, containing the following information:

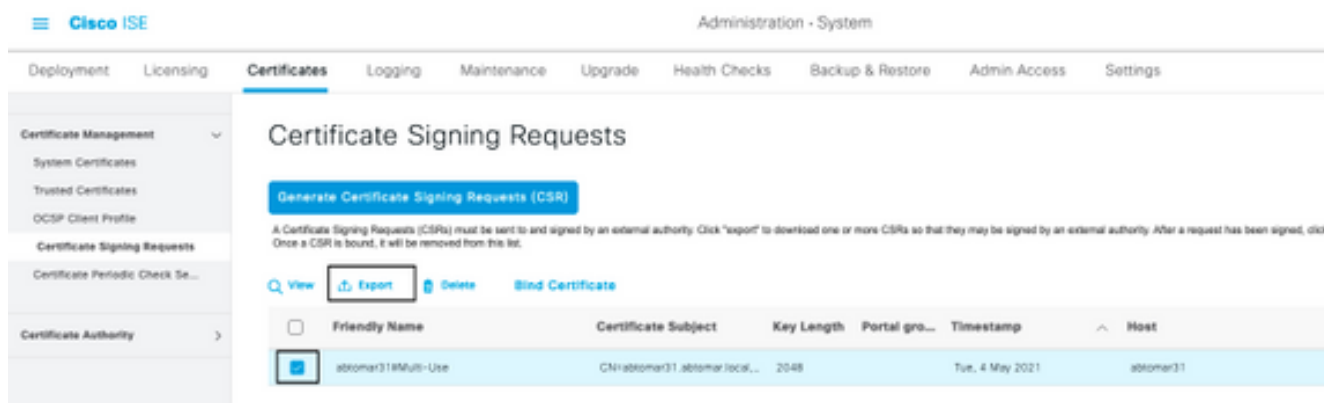
Field	Value
# address	10.126.129.85
DNS Name	abcdns01.abcdns.local

The 'Generate' button is also highlighted with a red box.

3. [Subject Alternative Name (SAN)] テキスト フィールド行の 1 つで、ISE FQDN を繰り返す必要があります。代行名またはワイルドカード証明書を使用する場合、2 つ目の SAN フィールドを追加できます。
4. [Generate] をクリックすると、ポップアップウィンドウに CSR フィールドが正しく入力されているかどうかが表示されます。



5. CSR をエクスポートするために、左側のパネルで [Certificate Signing Requests] をクリックし、CSR を選択し、[Export] をクリックします。



6. CSRはコンピュータに保存されます。それを署名用に CA に送信します。

証明書のインストール

CA から最終的な証明書を受信したら、その証明書を ISE に追加する必要があります。

1. ISE コンソールで、[Administration] > [System] > [Certificates] > [Certificate Signing Requests] に移動し、CRS のチェックボックスをオンにして [Bind Certificate] をクリックします。

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Se...

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Request (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, it will be removed from this list.

View Export Delete Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	abtomar31@Multi-Use	CN=abtomar31.abtomar.local...	2048		Tue, 4 May 2021	abtomar31

- [Friendly Name] テキストフィールドに証明書の簡単でわかりやすい説明を入力し、[Submit] をクリックします。

注：この時点では、EAP または Admin プロトコルを有効にしないでください。

- [System Certificate] の下に、次に示すように未使用の新しい証明書があります。

<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS4PH-CA	Tue, 4 May 2021	Thu, 4 May 2023
<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS4PH-CA	Tue, 4 May 2021	Thu, 4 May 2023

- 古い証明書が期限切れになる前に新しい証明書がインストールされるため、日付範囲の指定が未来になっていることを報告するエラーが表示されます。



- 継続するには [Yes] をクリックします。緑色で強調表示されているように、これで証明書はインストールされましたが、使用中にはなっていません。

<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS4PH-CA	Tue, 4 May 2021	Thu, 4 May 2023	
<input type="checkbox"/>	Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Wed, 5 May 2021

注：分散導入で自己署名証明書を使用する場合は、プライマリ自己署名証明書をセカンダリ ISE サーバの信頼できる証明書ストアにインストールする必要があります。同様に、セカンダリ自己署名証明書をプライマリ ISE サーバの信頼できる証明書ストアにインストールする必要があります。これにより、ISE サーバは相互に認証できます。これがないと、導入が中断する可能性があります。サードパーティ CA から証明書を更新する場合は、ルート証明書チェーンが変更されているかどうかを確認し、それに応じて ISE 内の信頼できる証明書ストアを更新します。両方のシナリオで、ISE ノード、エンドポイント制御システム、サブリカントがルート証明書チェーンを検証できることを確認します。

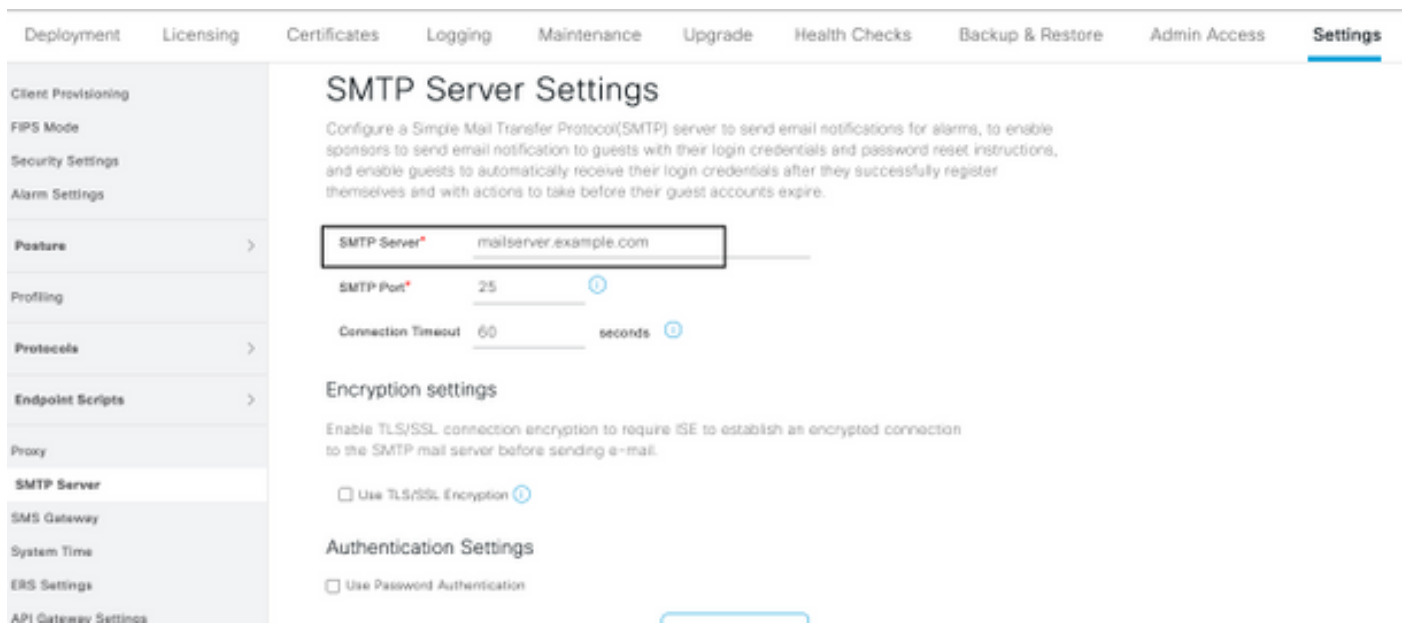
警告システムの設定

Cisco ISE はローカル証明書の失効日が 90 日以内に迫ったときに通知します。このような事前通知により、証明書の期限切れを回避して、証明書の更新を計画し、ダウンタイムを阻止または最小限に抑えることができます。

この通知はいくつかの方法で表示されます。

- 色づけされた有効期限のステータスのアイコンが、[Local Certificates] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 期限切れアラームは、期限切れの 90 日前と 60 日前に生成されたあと、期限切れ前の 30 日間は毎日生成されます。

期限切れアラームの電子メール通知を行うように ISE を設定します。ISE コンソールで、[Administration] > [System] > [Settings] > [SMTP Server] に移動して、Simple Mail Transfer Protocol (SMTP) サーバを特定し、アラームの電子メール通知が送信されるようにその他のサーバ設定を定義します。



The screenshot shows the Cisco ISE Settings page for SMTP Server configuration. The navigation bar includes Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The left sidebar lists various settings categories, with SMTP Server selected. The main content area is titled 'SMTP Server Settings' and includes a description: 'Configure a Simple Mail Transfer Protocol(SMTP) server to send email notifications for alarms, to enable sponsors to send email notification to guests with their login credentials and password reset instructions, and enable guests to automatically receive their login credentials after they successfully register themselves and with actions to take before their guest accounts expire.' The configuration fields are: SMTP Server (mailserver.example.com), SMTP Port (25), and Connection Timeout (60 seconds). There are also sections for Encryption settings (Use TLS/SSL Encryption) and Authentication Settings (Use Password Authentication).

通知をセットアップするには、次の 2 つの方法があります。

- 管理者に通知するには、管理者アクセスを使用します。

[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Users] に移動します。

アラーム通知を受信する必要がある管理者ユーザの [Include system alarms in emails] チェックボックスをオンにします。アラーム通知の送信者の電子メール アドレスは `ise@hostname` としてハードコードされています。

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Authentication
Authorization >
Administrators >
Admin Users
Admin Groups
Settings >

Admin User

* Name admin

Status Enabled

Email admin@example.com Include system alarms in emails

External

Change Password

Read Only

Inactive account never disabled

> User Information

> Account Options

Admin Groups

* Super Admin

- ユーザに通知するには、ISE アラーム設定を構成します。

下図に示す [Administration] > [System] > [Settings] > [Alarm Settings] > [Alarm Configuration] に移動します。

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Client Provisioning
RFS Mode
Security Settings
Alarm Settings
Policies >
Profiling
Protocols >
Endpoint Settings >
Pools
SMTP Server
SMS Gateway
System Time
DNS Settings
API Gateway Settings
Network Business Strategist >
DHCP & DNS Services
Web Services
Light Data Distribution
Interactive Help

Alarm Settings

Alarm Configuration Alarm Notification

Full Add Delete

Alarm Name	Category	Severity	Status	User Defined
<input type="radio"/> OS Server is down	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> OS Server is up	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> OSA Failed	BI Services		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> OSA Network Failed	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Expiration	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Expired	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Expiry Imminent Error	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Replication Failed	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Replication Temporarily Failed	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate Revoked	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Certificate required Synchronization failed	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/> Cisco profile applied to all devices	Administrative and Operational Audit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

注：アラームを発生させたくないカテゴリのステータスを無効にします。[Certificate Expiration] を選択して、[Alarm Notification] をクリックし、通知先のユーザーの電子メールアドレスを入力して、設定変更を保存します。変更がアクティブになるまでに最大15分かかる場合があります。

Alarm Settings

Alarm Configuration

Alarm Notification

Alarm Name: Certificate Expiration

Description: This certificate will expire soon. When it expires, ISE may fail when attempting to establish secure communications with clients. Inter-node communication may also be affected

Suggested Actions: Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can just delete the certificate if it is no longer used

Status: Enable

Severity: WARNING

Send Syslog Message

Enter multiple e-mails separated with comma: admin@abtomar.com

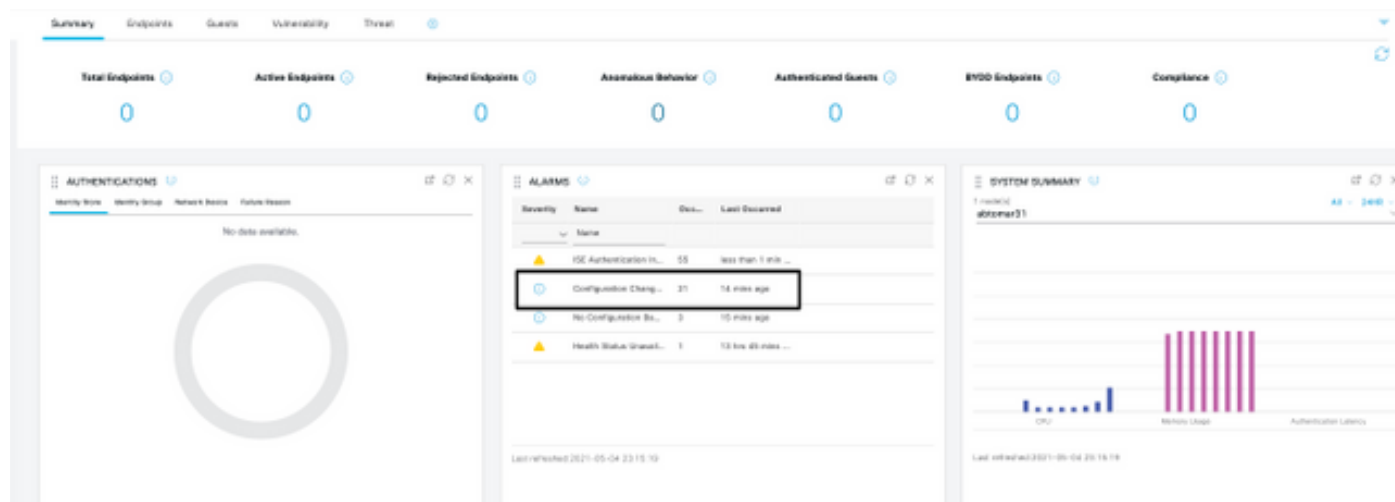
Notes in Email (0 to 4000 characters)

確認

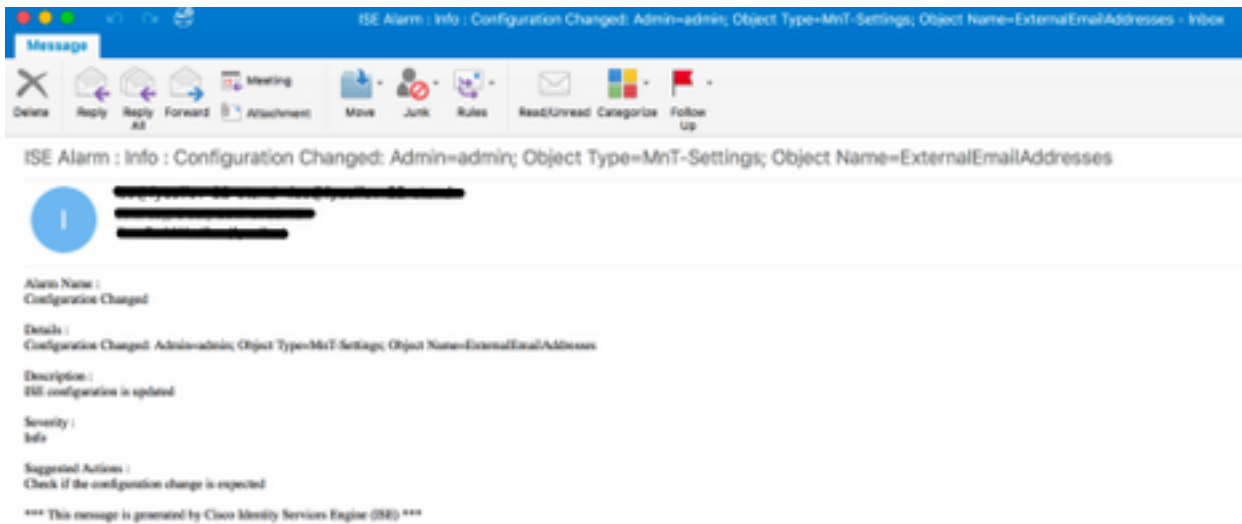
ここでは、設定が正常に機能しているかどうかを確認します。

警告システムの確認

警告システムが正しく機能していることを確認します。この例では、設定の変更によって、情報の重大度を含むアラートが生成されます（情報アラームが最も低い重大度ですが、証明書の期限切れはそれよりも高い重大度である警告を生成します）。



ISE から送信される電子メール アラームの例を以下に示します。



証明書変更の確認

この手順では、証明書が正しくインストールされていることを確認する方法、およびEAPや管理者の役割を変更する方法について説明します。

1. ISE コンソールで [Administration] > [Certificates] > [System Certificates] に移動し、新しい証明書を選択して、詳細情報を表示します。

注意： Admin の使用を有効にすると、ISE サービスが再起動するため、サーバーのダウンタイムが発生します。

Issuer	
* Friendly Name	AdminISE
Description	
Subject	CN=abtomar31.abtomar.local,OU=cisco
Subject Alternative Name (SAN)	IP Address: 10.106.120.85 DNS Name: abtomar31.abtomar.local
Issuer	abtomar-WIN-231PNBS4PH-CA
Valid From	Tue, 4 May 2021 21:00:34 IST
Valid To (Expiration)	Thu, 4 May 2023 21:00:34 IST
Serial Number	22 00 00 00 11 D8 BC 40 BD 11 C0 68 3E 00 00 00 00 11
Signature Algorithm	SHA256WITHRSA
Key Length	2048
Certificate Policies	

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- peGrid: Use certificate for the peGrid Controller
- ISE Messaging Service: Use certificate for the ISE Messaging Service
- EAP: Use certificate for EAP: Server

2. ISE サーバ上の証明書ステータスを確認するために、次のコマンドを CLI に入力します。

```
CLI:> show application status ise
```

3. すべてのサービスがアクティブになったら、管理者としてログインします。
4. 分散導入シナリオの場合は、[Administration] > [System] > [Deployment] に移動します。ノードに緑色のアイコンがあることを確認します。アイコンの上にカーソルを置き、凡例に「Connected」と表示されていることを確認します。
5. エンドユーザー認証が成功することを確認します。これを行うには、[Operations] > [RADIUS] > [Livelogs]に移動します。 特定の認証試行を検索し、それらの試行が正常に認証されたことを確認できます。

証明書の確認

証明書を外部からチェックする場合は、組み込みの Microsoft Windows ツールまたは OpenSSL ツールキットを使用します。

OpenSSL はセキュア ソケット レイヤ (SSL) プロトコルのオープン ソース実装です。証明書で独自のプライベート CA が使用されている場合は、ローカル マシンにルート CA 証明書を配置して、OpenSSL オプション `-CApath` を使用する必要があります。中間 CA が存在する場合は、それも同じディレクトリに配置する必要があります。

証明書に関する一般情報を取得してそれを検証するには、以下を使用します。

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

また、OpenSSL ツールキットを使用して証明書を変換することも役立ちます。

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

トラブルシューティング

現在、この設定に関する特定の診断情報はありません。

結論

アクティブになる前に新しい証明書を ISE にインストールできるため、古い証明書が期限切れになる前に新しい証明書をインストールすることをお勧めします。古い証明書の失効日と新しい証明書の開始日の間の重複期間が、証明書を更新してそれらのインストールを最小限のダウンタイムでまたはダウンタイムなしで計画するための時間になります。新しい証明書が有効な日付範囲に入ったら、EAP が Admin または両方を有効にします。Admin の使用を有効にすると、サービスが再起動されることに注意してください。

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。