

# Configurazione dei rinnovi dei certificati in ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Visualizzare i certificati autofirmati ISE](#)

[Stabilire quando modificare il certificato](#)

[Generare la richiesta di firma del certificato](#)

[Installare il certificato](#)

[Configurare il sistema di allarmi](#)

[Verifica](#)

[Verificare il sistema di avvisi](#)

[Verificare la modifica al certificato](#)

[Verificare il certificato](#)

[Risoluzione dei problemi](#)

[Conclusioni](#)

## Introduzione

In questo documento vengono descritte le best practice e le procedure proattive per rinnovare i certificati su Cisco ISE (Identity Services Engine). Viene inoltre esaminato come impostare avvisi e notifiche in modo che gli amministratori vengano avvisati di eventi imminenti, ad esempio la scadenza dei certificati.

**Nota:** Questo documento non è da considerarsi una guida diagnostica per i certificati.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Certificati X509
- Configurazione di un Cisco ISE con i certificati

### Componenti usati

"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".

- Cisco ISE Release 3.0.0.458
- Appliance o VMware

## Premesse

Gli amministratori ISE devono saper gestire i certificati ISE in scadenza. Se il certificato del server ISE è scaduto, possono verificarsi problemi gravi a meno che il certificato scaduto non venga sostituito con un nuovo certificato valido.

**Nota:** Se il certificato utilizzato per il protocollo EAP (Extensible Authentication Protocol) scade, è possibile che tutte le autenticazioni abbiano esito negativo perché i client non considerano più attendibile il certificato ISE. Se il certificato di amministrazione ISE scade, il rischio è ancora maggiore: un amministratore non sarà più in grado di accedere all'ISE e l'implementazione distribuita può cessare di funzionare e di replicarsi.

L'amministratore ISE deve installare un nuovo certificato valido sull'ISE prima della scadenza del vecchio certificato. Questo approccio proattivo previene o riduce al minimo le interruzioni dell'operatività senza conseguenze sugli utenti finali. Una volta iniziato il periodo di tempo del nuovo certificato installato, è possibile abilitare EAP/Admin o qualsiasi altro ruolo sul nuovo certificato.

È possibile configurare ISE in modo che generi allarmi e notifiche che avvisano l'amministratore di installare i certificati nuovi prima della scadenza dei certificati esistenti.

**Nota:** Questo documento utilizza il certificato ISE Admin come certificato autofirmato per dimostrare l'impatto del rinnovo del certificato, ma questo approccio non è consigliato per un sistema di produzione. È preferibile utilizzare un certificato CA per entrambi i ruoli EAP e Admin.

## Configurazione

### Visualizzare i certificati autofirmati ISE

Al momento dell'installazione, ISE genera un certificato autofirmato. Il certificato autofirmato viene usato per l'accesso amministrativo e per comunicare all'interno dell'implementazione distribuita (HTTPS) o per l'autenticazione degli utenti (EAP). Se il sistema è operativo, usare un certificato CA anziché un certificato autofirmato.

**Suggerimento:** per ulteriori informazioni, fare riferimento alla sezione [Gestione dei certificati in Cisco ISE](#) nella [Guida all'installazione dell'hardware Cisco Identity Services Engine, Release 3.0](#).

Il formato di un certificato ISE deve essere Privacy Enhanced Mail (PEM) o Distinguished

Encoding Rules (DER).

Per visualizzare il certificato autofirmato iniziale, andare a **Administration > System > Certificates > System Certificates** (Amministrazione > Sistema > Certificati > Certificati di sistema) nella GUI dell'ISE, come mostrato in questa immagine.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
<input type="checkbox"/>	OU=ISE Messaging Service,CN=abtomar31.abtomar.local#Certificate Services Endpoint Sub CA - abtomar31#00001	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#Certificate Services Endpoint Sub CA - abtomar31#00002	pxGrid		abtomar31.abtomar.local	Certificate Services Endpoint Sub CA - abtomar31	Mon, 3 May 2021	Mon, 4 May 2026	●
<input type="checkbox"/>	Default self-signed SAML 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	●

Se si installa un certificato server sull'ISE tramite una richiesta di firma del certificato, o CSR (Certificate Signing Request), e modificare il certificato del protocollo Admin o EAP. Il certificato server autofirmato è ancora presente ma lo stato è Not in-use (Non in uso).

**Attenzione:** per le modifiche al protocollo Admin, è necessario riavviare i servizi ISE e prevedere alcuni minuti di interruzione dell'operatività. Le modifiche al protocollo EAP non attivano il riavvio dei servizi ISE e non causano interruzioni dell'operatività.

## Stabilire quando modificare il certificato

Si supponga che il certificato installato sia in scadenza. È preferibile lasciare scadere il certificato prima di rinnovarlo o modificarlo prima della scadenza? È necessario modificare il certificato prima della scadenza in modo da avere il tempo di pianificare lo scambio del certificato e gestire eventuali tempi di inattività causati dallo scambio.

Quando è necessario modificare il certificato? Richiedere un nuovo certificato con una data di inizio antecedente alla data di scadenza del vecchio certificato. La differenza tra le due date viene chiamato intervallo di modifica.

**Attenzione:** se si abilita Admin, il servizio viene riavviato sul server ISE e si verificano alcuni minuti di interruzione dell'operatività.

Questa immagine mostra le informazioni di un certificato in scadenza:

<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 ⚠
--------------------------	--	--	------------------------------------	-------------------------	-------------------------	-----------------	-------------------

## Generare la richiesta di firma del certificato

Questa procedura descrive come rinnovare il certificato inviando una richiesta CSR:

1. Sulla console dell'ISE, andare a **Administration > System > Certificates > Certificate Signing Requests** (Amministrazione > Sistema > Certificati > Richieste di firma del certificato) e fare clic su **Generate Certificate Signing Request: (Genera richiesta di firma del certificato)**.
2. Nel campo di testo **Certificate Subject** (Oggetto del certificato), immettere almeno le informazioni **CN=ISEfqdn**, dove *ISEfqdn* è il nome di dominio completo, o FQDN (Fully Qualified Domain Name), dell'ISE. Aggiungere ulteriori campi come O (Organizzazione), OU (Unità organizzativa) o C (Paese) nell'oggetto del certificato usando le virgole:

The screenshot shows the Cisco ISE Administration console interface. The page title is "Administration - System". The navigation menu on the left includes "Certificates" which is currently selected. The main content area is titled "Notes" and contains a table with the following data:

Name	CSR Ready State
allse011	allse011 CSR not gen

Below the table is the "Subject" section with the following fields:

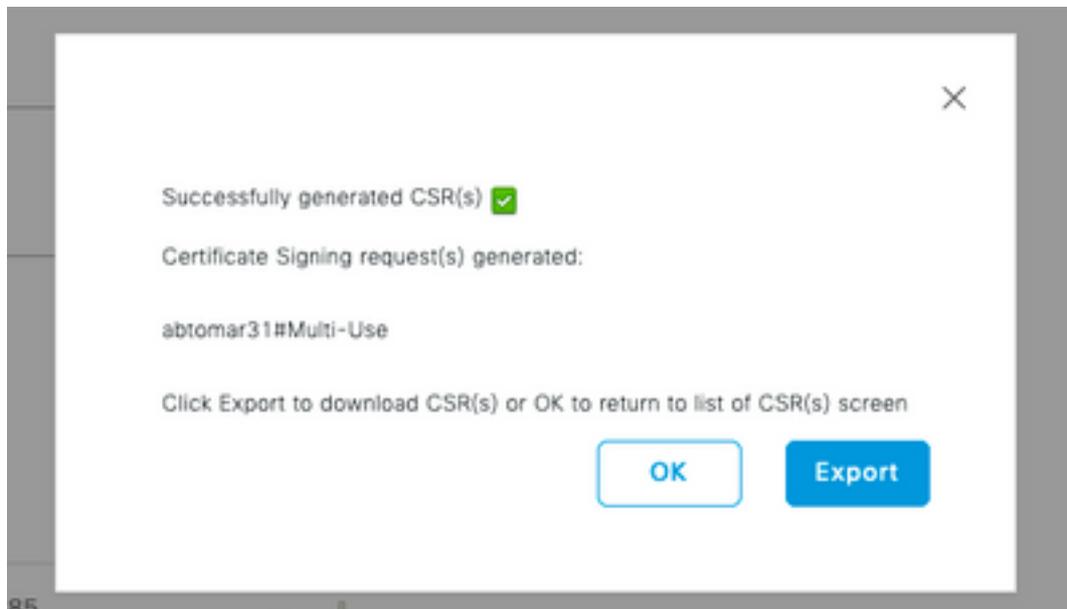
- Common Name (CN): ISEfqdn
- Organization (O):
- Organizational Unit (OU):
- Country (C):
- Email (E):

A red box highlights the "Subject Alternative Name (SAN)" section, which includes the following fields:

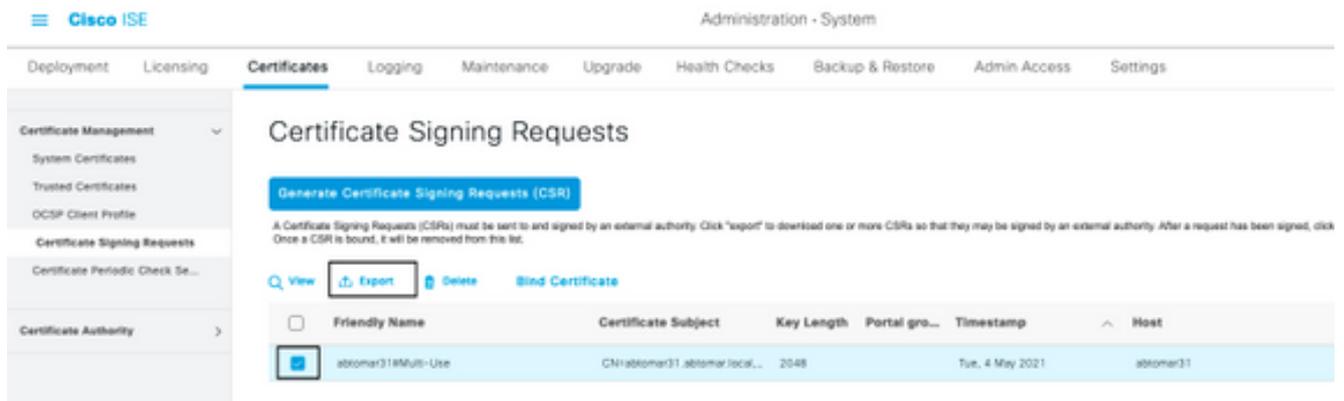
- IP address: 10.130.129.85
- DNS Name: allse011.allse011.local

At the bottom right of the page, there is a "Generate" button and a "Cancel" button, both highlighted with red boxes.

3. Su una delle righe del campo di testo **Subject Alternative Name (SAN)** (Nome alternativo del soggetto), ripetere il nome FQDN dell'ISE. È possibile aggiungere un secondo campo SAN se si desidera utilizzare nomi alternativi o un certificato con caratteri jolly.
4. Fare clic su **Generate** (Genera), una finestra a comparsa mostra se i campi CSR sono stati compilati correttamente:



- Per esportare la richiesta CSR, fare clic su **Certificate Signing Requests** (Richieste di firma del certificato) nel pannello a sinistra, selezionare CSR, quindi fare clic su **Export** (Esporta):



- Il CSR è memorizzato nel computer. Inviarla all'autorità di certificazione (CA) per la firma.

## Installare il certificato

Dopo aver ricevuto il certificato finale dalla CA, è necessario aggiungere il certificato all'ISE:

- Sulla console ISE, andare a **Administration > System > Certificates > Certificate Signing Requests** (Amministrazione > Sistema > Certificati > Richieste di firma del certificato), quindi selezionare la casella di controllo CRS e fare clic su **Bind Certificate** (Associa certificato):

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 Authority

## 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"/>	abtomar31Multi-Use	CN=abtomar31.abtomar.local...	2048		Tue, 4 May 2021	abtomar31

- Immettere una descrizione semplice e chiara del certificato nel campo di testo **Friendly Name** (Nome descrittivo) e fare clic su Submit (Invia).

**Nota:** non abilitare il protocollo EAP o Admin in questa fase.

- In System Certificate (Certificato di sistema), viene visualizzato un nuovo certificato con lo stato Not in use (Non in uso), come mostrato qui:

<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"/>						

- Poiché il nuovo certificato viene installato prima che il certificato precedente scada, viene visualizzato un errore che segnala un intervallo di date future:

**The certificate you are importing has a date range in the future - it is not yet valid. Are you sure you want to continue?**

Yes No

- Fare clic su **Yes** (Sì) per continuare. Il certificato è ora installato ma non in uso, come evidenziato dal riquadro verde.

<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

**Nota:** se si usano i certificati autofirmati in un'implementazione distribuita, il certificato autofirmato principale deve essere installato nell'archivio dei certificati attendibili sul server ISE secondario. Analogamente, il certificato autofirmato secondario deve essere installato nell'archivio dei certificati attendibili del server ISE principale. Ciò consente l'autenticazione reciproca dei server ISE. In caso contrario, l'installazione potrebbe interrompersi. Se si rinnovano i certificati di una CA di terze parti, verificare se la catena dei certificati radice è cambiata e aggiornare di conseguenza l'archivio dei certificati attendibili nell'ISE. In entrambi

gli scenari, verificare che i nodi ISE, i sistemi di controllo degli endpoint e i supplicant siano in grado di convalidare la catena di certificati radice.

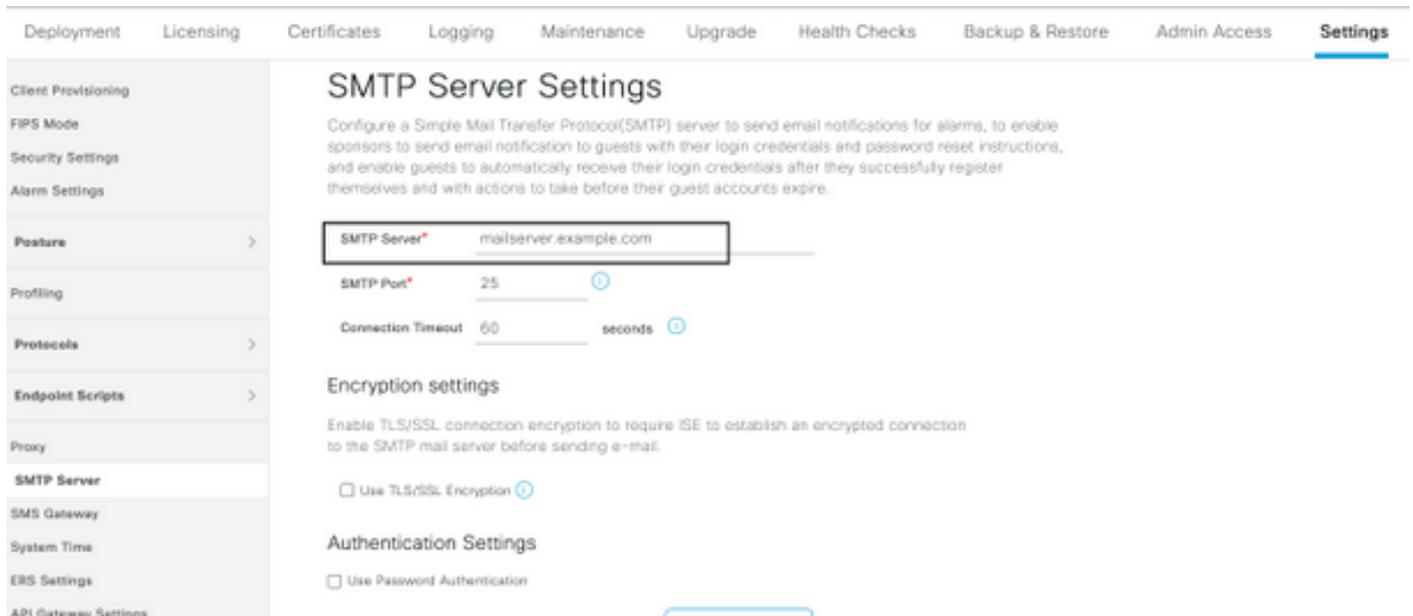
## Configurare il sistema di allarmi

Cisco ISE avvisa l'utente quando un certificato locale scade entro 90 giorni. Tale notifica anticipata permette di evitare che i certificati scadano, pianificare eventuali modifiche e prevenire o ridurre al minimo l'interruzione dell'operatività.

La notifica viene visualizzata in diversi modi:

- Icone di stato colorate visualizzate nella pagina Local Certificates (Certificati locali).
- Messaggi di scadenza visualizzati nel report di diagnostica del sistema Cisco ISE.
- Avvisi di scadenza generati a 90 giorni e a 60 giorni, quindi ogni giorno negli ultimi 30 giorni prima della scadenza.

Configurare ISE in modo che gli avvisi di scadenza vengano notificati tramite e-mail. Sulla console ISE, andare a **Administration > System > Settings > SMTP Server** (Amministrazione > Sistema > Impostazioni > Server SMTP), individuare il server Simple Mail Transfer Protocol (SMTP) e definire le altre impostazioni del server in modo da inviare le notifiche tramite e-mail:



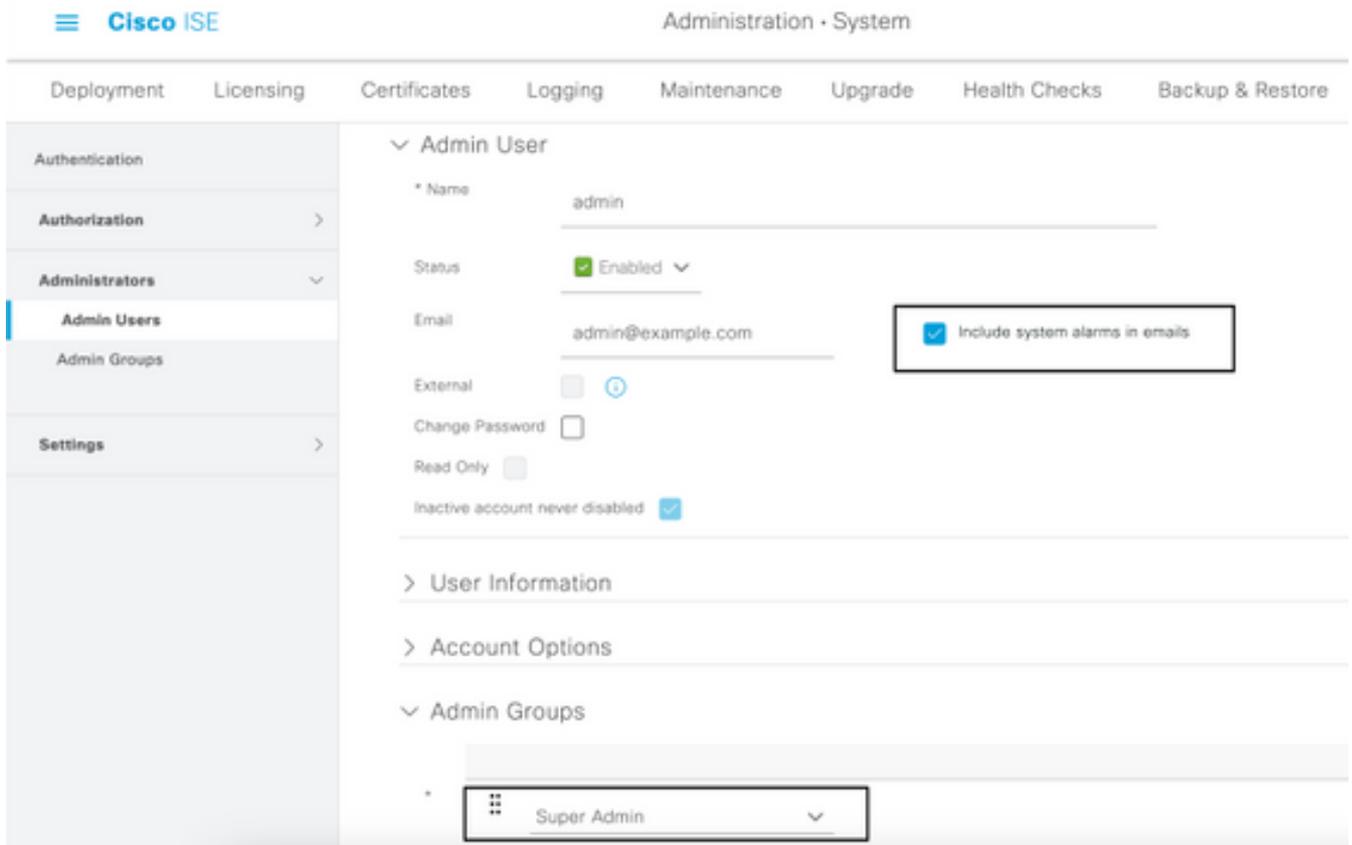
The screenshot shows the 'SMTP Server Settings' configuration page in the Cisco ISE administration console. The page is divided into a left sidebar with navigation options and a main content area. The main content area includes a description of the SMTP server's role, input fields for 'SMTP Server' (set to 'mailserver.example.com'), 'SMTP Port' (set to 25), and 'Connection Timeout' (set to 60 seconds). Below these are sections for 'Encryption settings' and 'Authentication Settings', both with checkboxes for 'Use TLS/SSL Encryption' and 'Use Password Authentication' respectively.

È possibile impostare le notifiche in due modi:

- Tramite l'accesso Admin per le notifiche agli amministratori:

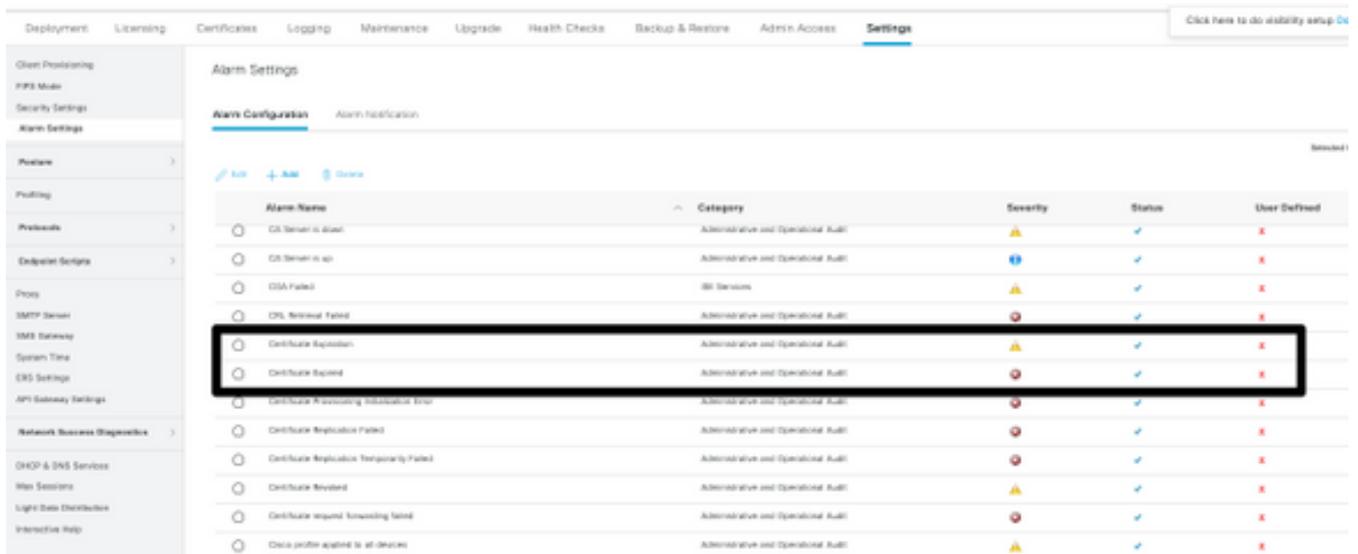
Andare a **Administration > System > Admin Access > Administrators > Admin Users** (Amministrazione > Sistema > Accesso amministratore > Amministratori > Utenti amministratori).

Selezionare la casella di controllo **Include system alarms in emails** (Includi avvisi di sistema nelle e-mail) per ricevere notifiche. L'indirizzo e-mail del mittente delle notifiche di allarme è codificato come `ise@hostname`.



- Configurare le impostazioni di allarme ISE per inviare notifiche agli utenti:

Andare a **Administration > System > Settings > Alarm Settings > Alarm Configuration** (Amministrazione > Sistema > Impostazioni > Impostazioni allarme > Configurazione allarmi), come mostrato nell'immagine.



**Nota:** disabilitare lo stato di una categoria per escludere la generazione di allarmi per tale categoria. Selezionare Certificate Expiration (Scadenza certificati), quindi fare clic su **Alarm**

**Notification** (Notifica allarmi), immettere gli indirizzi e-mail degli utenti a cui inviare gli avvisi e salvare le modifiche alla configurazione. Le modifiche possono richiedere fino a 15 minuti prima che siano attive.

## 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

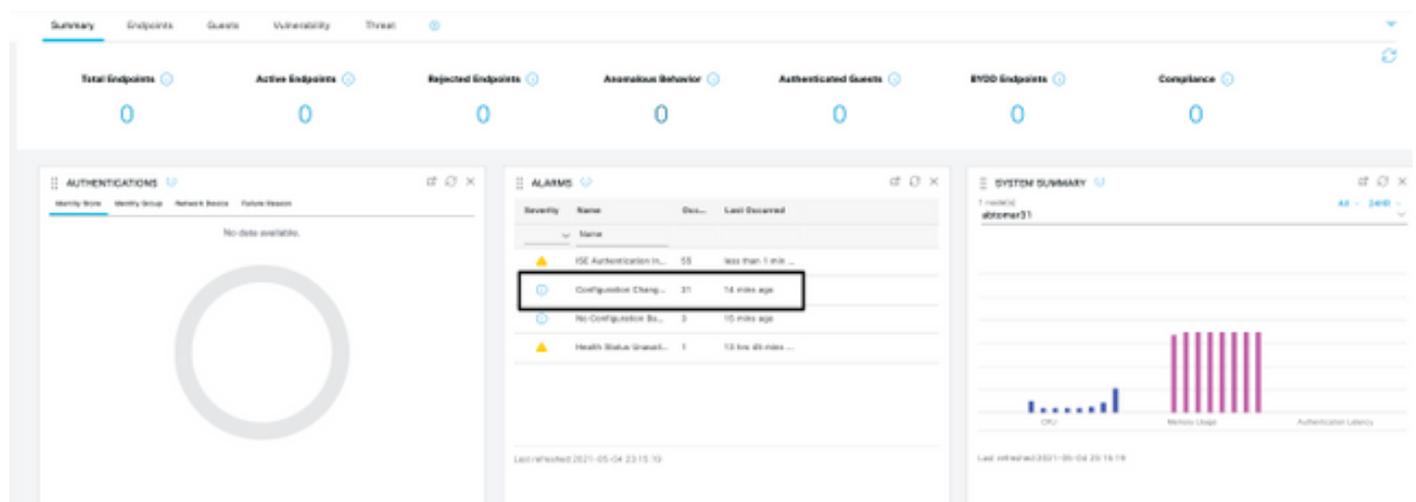
Notes in Email (0 to 4000 characters)

## Verifica

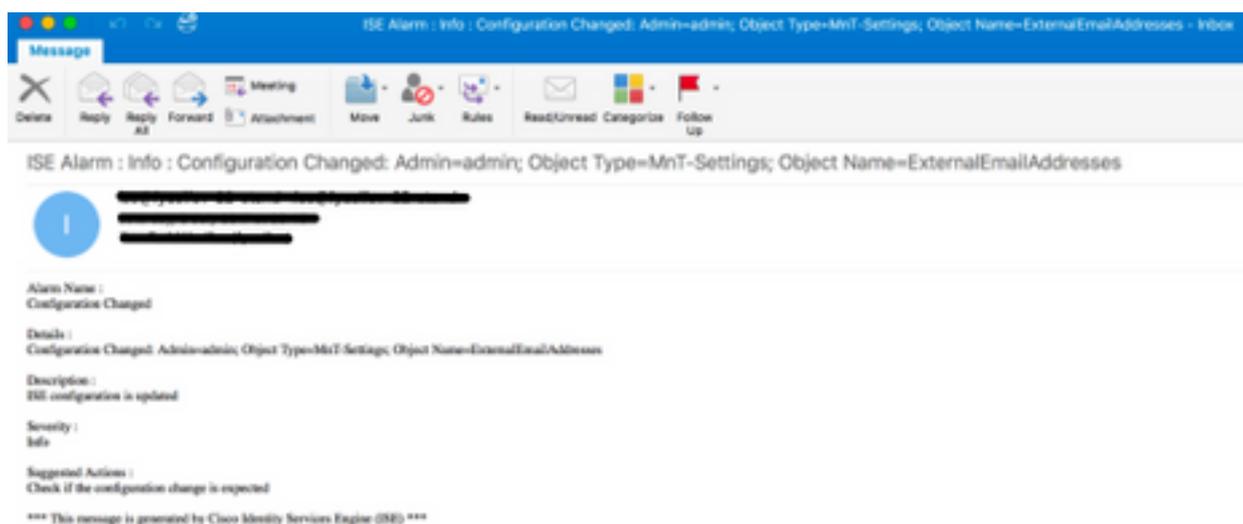
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

### Verificare il sistema di avvisi

Verificare che il sistema di avvisi funzioni correttamente. In questo esempio, una modifica alla configurazione genera un avviso con un livello di gravità Information (Avviso informativo). (Un avviso informativo ha la gravità più bassa; quando il certificato scade, il livello di gravità è più elevato.)



Ecco un esempio dell'allarme e-mail inviato da ISE:



## Verificare la modifica al certificato

In questa procedura viene descritto come verificare che il certificato sia installato correttamente e come modificare i ruoli EAP e/o Admin:

1. Sulla console ISE, andare a **Administration > Certificates > System Certificates** (Amministrazione > Certificati > Certificati di sistema) e selezionare il nuovo certificato per visualizzare i dettagli.

**Attenzione:** se si abilita l'utilizzo da parte dell'amministratore, il servizio ISE viene riavviato, causando l'interruzione dell'operatività del server.

The screenshot shows the Cisco ISE Administration interface. A warning dialog box is displayed in the foreground, stating: "Warning: Enabling Admin role for this certificate will cause an application server restart on the selected node." The dialog has "OK" and "Cancel" buttons. In the background, the "Certificates" page is visible, showing details for an issuer named "AdminISE". The details include: 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 8C 40 BD 11 C0 6B 3E 00 00 00 00 11), Signature Algorithm (SHA256WITHRSA), Key Length (2048), and Certificate Policies. The Usage section is also visible, with "Admin" checked and other options like "EAP Authentication", "RADIUS DTLS", "pxGrid", and "ISE Messaging Service" unchecked.

2. Per verificare lo stato del certificato sul server ISE, immettere questo comando nella CLI:

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

3. Una volta che tutti i servizi sono attivi, provare ad accedere come amministratore.

4. Per uno scenario di distribuzione distribuita, selezionare **Amministrazione > Sistema > Distribuzione**. Verificare che il nodo disponga di un'icona verde. Posizionare il cursore sull'icona per verificare che la legenda indichi "Connesso".

5. Controllare che l'autenticazione dell'utente finale sia corretta. A tale scopo, selezionare **Operazioni > RAGGIO > Livelogs**. È possibile trovare un tentativo di autenticazione specifico e verificare che sia stato autenticato correttamente.

## Verificare il certificato

Se si desidera controllare il certificato esternamente, è possibile usare gli strumenti Microsoft Windows integrati o il toolkit OpenSSL.

OpenSSL è un'implementazione open source del protocollo Secure Sockets Layer (SSL). Se i certificati usano un'autorità di certificazione privata, posizionare il certificato CA radice su una macchina locale e usare l'opzione OpenSSL `-CApath`. Se si usa una CA intermedia, inserirla nella stessa directory.

Per ottenere informazioni generali sul certificato e verificarle, usare:

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

Può inoltre essere utile convertire i certificati con il toolkit OpenSSL:

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

## Risoluzione dei problemi

Non sono attualmente disponibili informazioni di diagnostica specifiche per questa configurazione.

## Conclusioni

Poiché è possibile installare un nuovo certificato su ISE prima che sia attivo, Cisco consiglia di installare il nuovo certificato prima che il certificato precedente scada. Questo periodo di sovrapposizione tra la data di scadenza del vecchio certificato e la data di inizio del nuovo certificato dà il tempo di rinnovare i certificati e pianificare la loro installazione con interruzione dell'operatività minima. Dopo aver immesso il nuovo certificato nel relativo intervallo di date valido, abilitare il protocollo EAP e/o Admin. Ricordare che, se si abilita l'utilizzo del protocollo Admin, il servizio viene riavviato.

## 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).