

Risoluzione dei problemi relativi al certificato di amministratore ISE scaduto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Certificato di amministrazione ISE \(scaduto\)](#)

[Convalida stato certificato amministratore](#)

[Piano d'azione](#)

[Risoluzione dei problemi](#)

[Caso di utilizzo 1: Nodo secondario non registrato bloccato in stato distribuito \(ise-psn1\)](#)

[Convalida lo stato](#)

[Soluzione alternativa](#)

[Caso di utilizzo 2: Interfaccia grafica del nodo secondario non registrata non raggiungibile \(ise-psn2\)](#)

[Convalida lo stato](#)

[Soluzione alternativa](#)

[Riferimenti](#)

[Pertinente](#)

Introduzione

In questo documento viene descritto come risolvere i problemi e rinnovare un certificato di amministratore Cisco Identity Services Engine (ISE) scaduto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Implementazione di Cisco ISE.
- Gestione certificati in Cisco ISE.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco Identity Services Engine (ISE) versione 3.3 Patch4.

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.

Premesse

Il presente documento si concentra sulla distribuzione; è tuttavia possibile utilizzare lo stesso piano di risoluzione dei problemi in un nodo autonomo.

In ISE Distributed Deployment, il nodo è PAN (Primary Admin Node) o secondario.

Questo documento utilizza il certificato ISE Admin come certificato autofirmato per dimostrare l'impatto del certificato scaduto, ma questo approccio non è consigliato per un sistema di produzione. È preferibile utilizzare un certificato firmato dall'autorità per l'utilizzo da parte dell'amministratore.



Nota: Cisco consiglia di mantenere il certificato amministratore in stato di integrità e di pianificare in anticipo il rinnovo. Questa guida consente di tenere traccia e rinnovare i certificati di sistema ISE ([configurare i rinnovi dei certificati sull'ISE](#)).

Certificato di amministrazione ISE (scaduto)

Convalida stato certificato amministratore

Passaggio 1. Controllare lo stato della distribuzione. Passare ad Amministrazione > Sistema > Distribuzione.

È possibile controllare lo stato dei nodi secondari, come mostrato, i tre nodi secondari sono (Non in sincronizzazione).

Identity Services Engine Administration / System

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

Deployment Nodes

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-psn1	Policy Service, pxGrid		SESSION, PROFILER	⚠ Not in Sync
ise-psn2	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	⚠

Stato distribuzione

Passo 2: esaminare gli allarmi. Passare a Pannello di controllo > Allarmi > (Certificato scaduto).

Per confermare il nodo e il certificato scaduto.

 Nota: Se il PAN (Primary Admin Node) è scaduto prima di qualsiasi nodo secondario, non è possibile visualizzare alcun allarme da quel nodo, è ciò che è accaduto per il SPAN (Secondary Admin Node) in questo allarme.

Identity Services Engine Alarms: Certificate Expired

Description

This certificate has expired! 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. For a system certificate, navigate to Administration > System > Certificate > System Certificates to view details. For a trusted certificate, navigate to Administration > System > Certificate > Trusted Certificates to view details

Rows/Page 3 |< < 1 / 1 > > Go 3 Total Rows

Time Stamp	Description	Details
Jan 23 2025 16:00:13.466 PM	Local certificate Default self-signed server certificate expired on Thu: 23 Jan 2025 Server=ise-ppan	
Jan 22 2025 16:37:23.498 PM	Local certificate Default self-signed server certificate expired on Thu: 23 Jan 2025 Server=ise-psn1	
Jan 22 2025 16:36:53.545 PM	Local certificate Default self-signed server certificate expired on Thu: 23 Jan 2025 Server=ise-psn2	

Avvisi (certificato scaduto)

Passaggio 3. Controllare lo stato del certificato di amministratore. Passare a Amministrazione > Sistema > Certificati > Gestione certificati > Certificati di sistema > Espandi nodo.

1. PAN (Primary Admin Node):

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node Restart

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdlab2.local	ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SA ML_ise-ppan.kdlab2.local	SAML		SAML_ise-ppan.kdlab2.local	SAML_ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-ppan#000003	pxGrid		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=ISE Messaging Service, OU=Certificate Services Endpoint Sub CA - ise-ppan#000004	ISE Messaging Service		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
> ise-psn1							
> ise-psn2							
> ise-span							

Stato certificato amministratore PPA

2. Nodi secondari.

Per i nodi secondari potrebbe essere disponibile una delle due opzioni e in entrambi i casi è necessario applicare lo stesso piano d'azione:

R. È possibile espandere il certificato di sistema del nodo e verificare che il certificato di amministrazione sia scaduto:

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node Restart

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

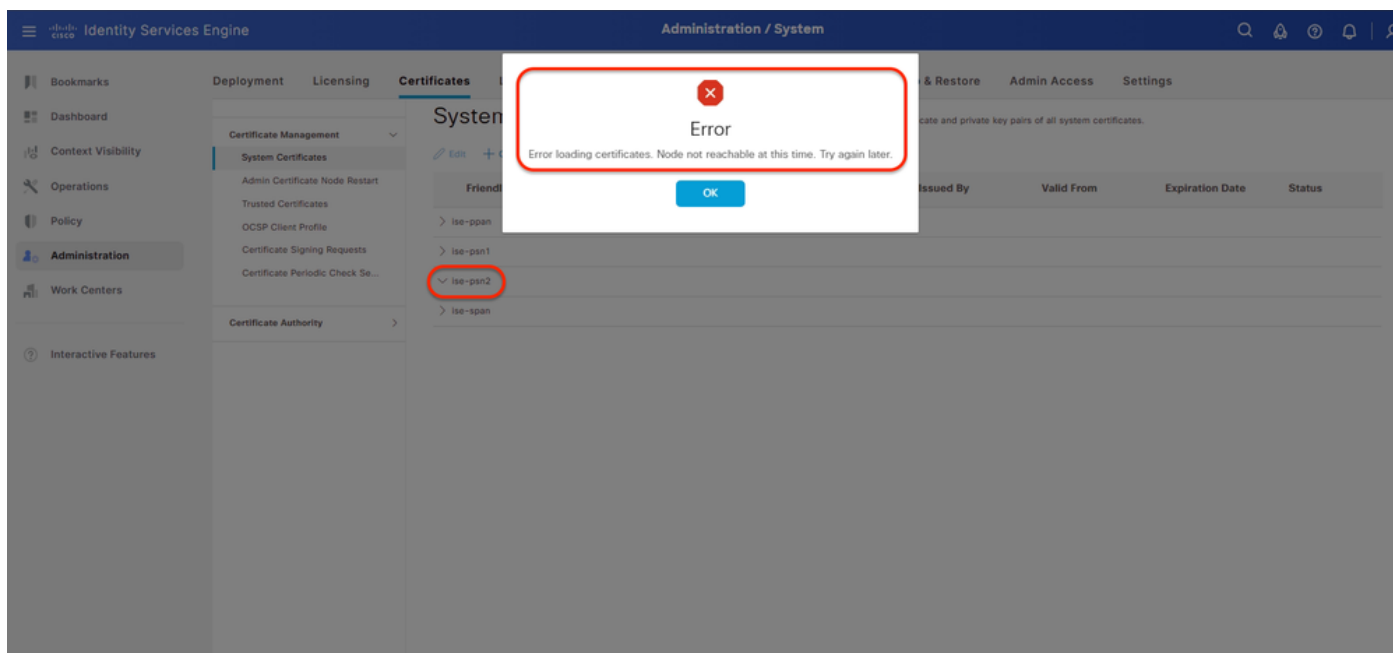
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
ise-psn1							
ise-psn2							
ise-span							
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SA ML_ise-ppan.kdlab2.local	SAML		SAML_ise-ppan.kdlab2.local	SAML_ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-span#000005	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service, OU=Certificate Services Endpoint Sub CA - ise-span#000006	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Stato certificato amministratore nodo secondario

B. Generare un errore ("Errore durante il caricamento dei certificati. Nodo non raggiungibile in questo momento. Riprovare più tardi.") come mostrato per (ise-psn2



Nodo secondario non raggiungibile

Piano d'azione

Dopo aver confermato che il certificato di amministratore è scaduto per tutti e 4 i nodi, è necessario eseguire la procedura seguente:

Passaggio 1. Annullare la registrazione di tutti i nodi secondari dalla distribuzione distribuita (solo se il certificato amministratore è scaduto).

Passare a Amministrazione > Sistema > Distribuzione > Controllo [✓] dei nodi secondari e fare clic su Annulla registrazione.

 **Nota:** Se si annulla la registrazione del nodo, questo verrà spostato in modalità autonoma e sarà possibile rinnovare il certificato di amministratore su questo nodo.

Deployment Nodes

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-pan1	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-pan2	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	⚠

Annulla registrazione nodi secondari

Nota: Annullare la registrazione solo dei nodi secondari in cui il certificato di amministratore è già scaduto e conservare gli altri. In questo documento, tutti i nodi secondari sono scaduti.

Deployment Nodes

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	✓

La registrazione di tutti i nodi secondari viene annullata

Passaggio 2. Rinnovare il certificato di amministratore del nodo di amministrazione principale (PPAN, Primary Admin Node).

1. Passare a Amministrazione > Sistema > Certificati > Gestione certificati > Certificati di sistema > Fare clic su +Genera certificato autofirmato:

Identity Services Engine Administration / System

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

Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit + Generate Self Signed Certificate Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdlab2.local	ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdlab2.local	SAML		SAML_ise-ppan.kdlab2.local	SAML_ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise-ppan#00003	pxGrid		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=ISE Messaging Service Ice#Certificate Services Endpoint Sub CA - ise-ppan#00004	ISE Messaging Service		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Genera nuovo certificato amministratore autofirmato

2. Selezionare il PPAN (Primary Admin Node) (ise-ppan) e immettere le informazioni sul certificato:

Identity Services Engine Administration / System

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

Certificate Management
System Certificates
Admin Certificate Node Restart
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node ise-ppan

Subject

Common Name (CN)
\$FQDN\$

Organizational Unit (OU)
Tech

Organization (O)
KD

City (L)

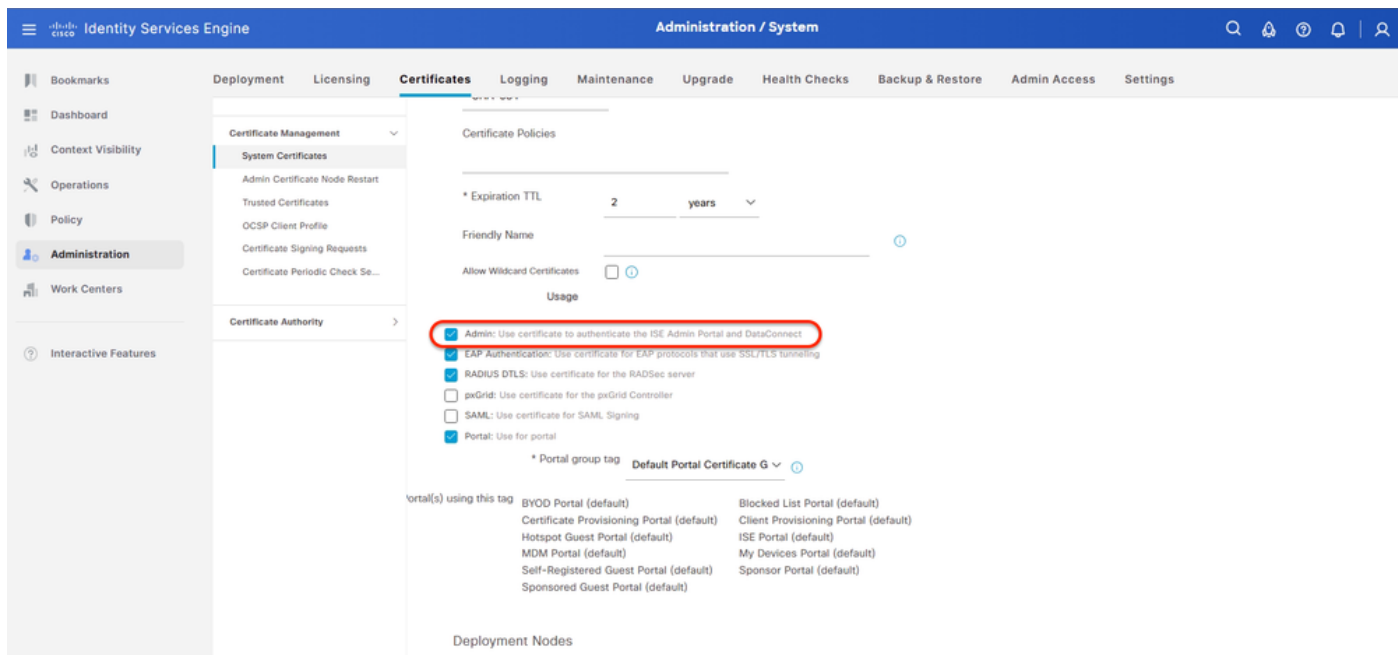
State (ST)

Country (C)

Subject Alternative Name (SAN)

Selezionare il PAN (Primary Admin Node)

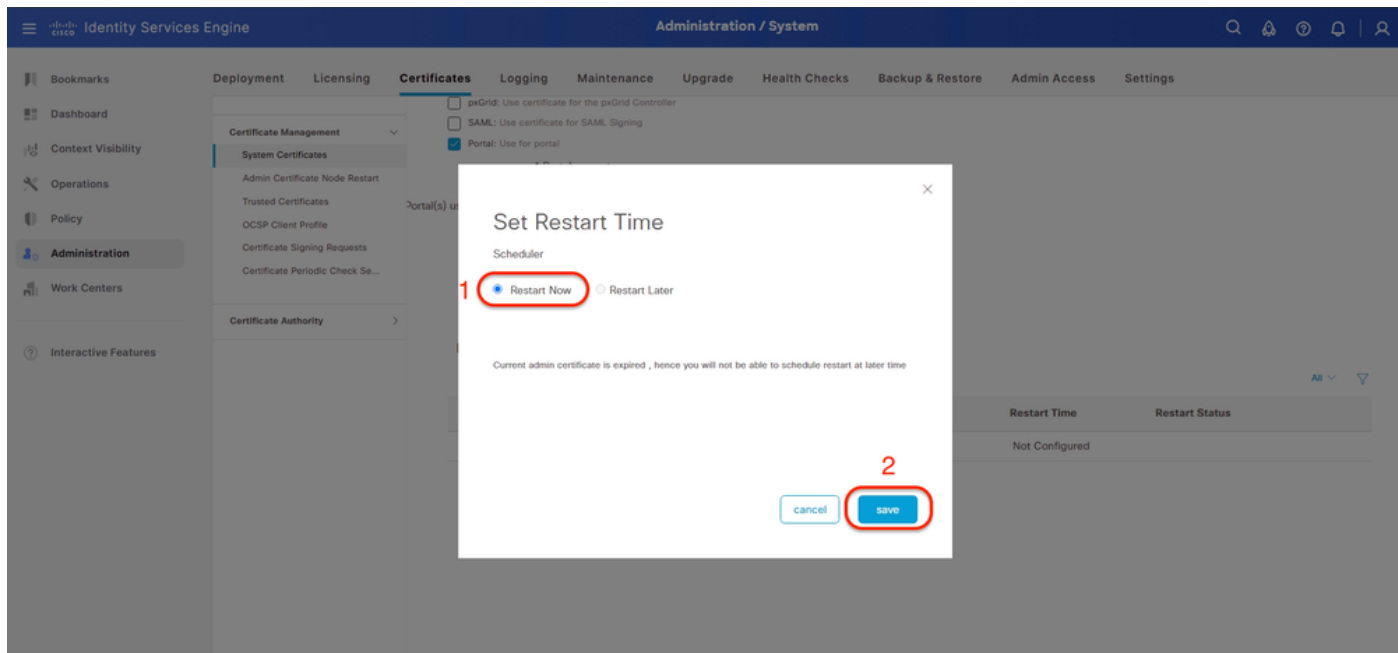
3. Selezionare [✓] l'utilizzo Admin.



Utilizzo amministratore

4. Impostare Restart Time (Ora di riavvio) su Restart Now (Riavvia ora) per il PAN (Primary Admin Node). Impostare tutti i nodi della distribuzione su Riavvia ora o Riavvia in seguito.

Dopo aver rinnovato un certificato di amministrazione (un certificato configurato per l'utilizzo da parte dell'amministratore) nel nodo di amministrazione primario (PAN), è necessario riavviare tutti i nodi della distribuzione.



Imposta ora di riavvio su Ora

5. Fare clic su Invia.

 Nota: Dopo aver rinnovato un certificato di amministrazione (un certificato configurato per l'utilizzo da parte dell'amministratore) nel nodo di amministrazione primario (PAN), è



necessario riavviare tutti i nodi della distribuzione. È possibile riavviare ogni nodo immediatamente oppure pianificare i riavvii in un secondo momento. Questa funzionalità consente di garantire che nessun processo in esecuzione venga interrotto dai riavvii automatici, offrendo un maggiore controllo sul processo.

È possibile visualizzare e modificare i riavvii pianificati nella finestra Amministrazione > Sistema > Certificati > Amministrazione - Riavvio nodo certificato, accessibile da Cisco ISE release 3.3.

6. Verificare il nuovo certificato di amministratore del PAN (Primary Admin Node).

Selezionare Amministrazione > Sistema > Certificati > Gestione certificati > Certificati di sistema > Espandi (ise-ppan).

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar contains navigation options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled 'System Certificates' and includes a table of certificates. The 'ise-ppan' certificate is highlighted with a red box. Below the table, a red box highlights the details of the 'ise-ppan' certificate.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Not in use		ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdiab2.local	SAML		SAML_ise-ppan.kdiab2.local	SAML_ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=Certificate Services, System Certificates, Certificate Services Endpoint Sub CA - ise-ppan#000003	peGrid		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=ISE Messaging Service, Certificate Services Endpoint Sub CA - ise-ppan#000004	ISE Messaging Service		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
O=KD, OU=Tech, CN=ise-ppan.kdiab2.local, OU=ise-ppan.kdiab2.local#000005	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active

Nuovo certificato amministratore (ise-ppan)

Passaggio 3. Rinnovare il certificato di amministratore dei nodi secondari.

1. Confermare il nodo secondario nella distribuzione autonoma dopo l'annullamento della registrazione nella distribuzione distribuita.

Cercare il nodo tramite GUI (<https://<FQDN/IP>>) e selezionare Amministrazione > Sistema > Distribuzione.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 0 Total 1

Hostnames	Personas	Role(s)	Services	Node Status
ise-span	Administration, Monitoring, Policy Service	STANDALONE	SESSION_PROFILER	✓

(ise-span) sull'installazione standalone

2. Passare ad Amministrazione > Sistema > Certificati > Gestione certificati > Certificati di sistema > Fare clic su +Genera certificato autofirmato.

Identity Services Engine Administration / System

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

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

+ Generate Self Signed Certificate + Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
CN=ise-span.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-span#00007	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service, OU=Certificate Services Endpoint Sub CA - ise-span#00008	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
Default self-signed saml server certificate - CN=SAML_ise-span.kdlab2.local	SAML		SAML_ise-span.kdlab2.local	SAML_ise-span.kdlab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Genera nuovo certificato amministratore autofirmato

3. Selezionare (ise-span) e immettere le informazioni sul certificato.

Identity Services Engine Administration / System

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node ise-span

Subject

Common Name (CN) SFQDN\$

Organizational Unit (OU) Tech

Organization (O) KQ

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

Selezionare il nodo

4. Selezionare [✓] l'utilizzo Admin.

Identity Services Engine Administration / System

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se...

Certificate Authority

* Digest to Sign With SHA-384

Certificate Policies

* Expiration TTL 2 years

Friendly Name

Allow Wildcard Certificates

Usage

☒ Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

☒ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

☒ RADIUS DTLS: Use certificate for the RADSec server

☐ pxGrid: Use certificate for the pxGrid Controller

☐ SAML: Use certificate for SAML Signing

☒ Portal: Use for portal

* Portal group tag Default Portal Certificate G

Portal(s) using this tag

BYOD Portal (default)	Blocked List Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	ISE Portal (default)
MDM Portal (default)	My Devices Portal (default)
Self-Registered Guest Portal (default)	Sponsor Portal (default)
Sponsored Guest Portal (default)	

Utilizzo amministratore

Nota: La modifica del certificato del ruolo di amministratore nel nodo ISE comporta il riavvio dei servizi.

5. Fare clic su Sottometti.

6. Verificare il nuovo certificato di amministratore su (ise-span).

Passa a Amministrazione > Sistema > Certificati > Gestione certificati > Certificati di sistema > Espandi (ise-span).

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Actions: Edit, Generate Self Signed Certificate, Import, Export, Delete, View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-span							
Default self-signed server certificate	Not in use		ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
O=ED, OU=Tech, CN=ise-span.kdlab2.local@ise-span.kdlab2.local#00009	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active
CN=ise-span.kdlab2.local, OU=Certificate Services System CertificateEndpoint Sub CA - Ise-span#00007	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - Ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service IseCertificate Services Endpoint Sub CA - Ise-span#00008	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - Ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
Default self-signed saml server certificate - CN=SAML_ise-span.kdlab2.local	SAML		SAML_ise-span.kdlab2.local	SAML_ise-span.kdlab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Nuovo certificato amministratore (ise-span)

Passaggio 4. Registrare i nodi secondari nella distribuzione distribuita.

Configurare i ruoli e gli utenti della distribuzione come prima (Admin, MNT, PSN, ecc.).

1. Dalla GUI del nodo di amministrazione principale (PPAN). Passare a Amministrazione > Sistema > Distribuzione > Fare clic su Registra.

Deployment Nodes

Selected 0 Total 1

Actions: Edit, Register, Sync, Deregister

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	Active

GUI PPAN (Primary Admin Node)

2. Immettere il nome di dominio completo e le credenziali del nodo secondario (nome utente/password).

Immettere il nome di dominio completo (FQDN) risolvibile DNS del nodo autonomo che si desidera registrare. Il nome di dominio completo (FQDN) della rete (PPAN) e il nodo da registrare devono

essere risolvibili l'uno dall'altro.

Identity Services Engine Administration / System

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

Deployment Nodes List > Specify Hostname

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*
ise-span.kdlab2.local

User Name*
admin

Password*

Next Cancel

Accesso al nodo secondario

3. Abilitare la persona e i servizi corretti.

Identity Services Engine Administration / System

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

Deployment Nodes List > Configure Node

Register ISE Node - Step 2: Configure Node

General Settings

Hostname ise-span

FQDN ise-span.kdlab2.local

IP Address

Node Type Identity Services Engine (ISE)

Role SECONDARY

Administration

Monitoring

Role PRIMARY

Other Monitoring Node ise-ppan

Dedicated MnT

Registra nodo secondario (ise-span)

Passaggio 5. Verificare lo stato della distribuzione.

Passare a Amministrazione > Sistema > Distribuzione.

Identity Services Engine Administration / System

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Deployment Nodes

Selected 0 Total 2

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓

(ise-span) Aggiunto all'implementazione

Risoluzione dei problemi

Caso di utilizzo 1: Nodo secondario non registrato bloccato in stato distribuito (ise-psn1)

Convalida lo stato

Passaggio 1. Confermare lo stato della distribuzione distribuita.

Dalla GUI del nodo di amministrazione principale (PPAN). Passare a Amministrazione > Sistema > Distribuzione. È possibile verificare che questo nodo (ise-psn1) sia già stato rimosso dalla registrazione.

Identity Services Engine Administration / System

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Deployment Nodes

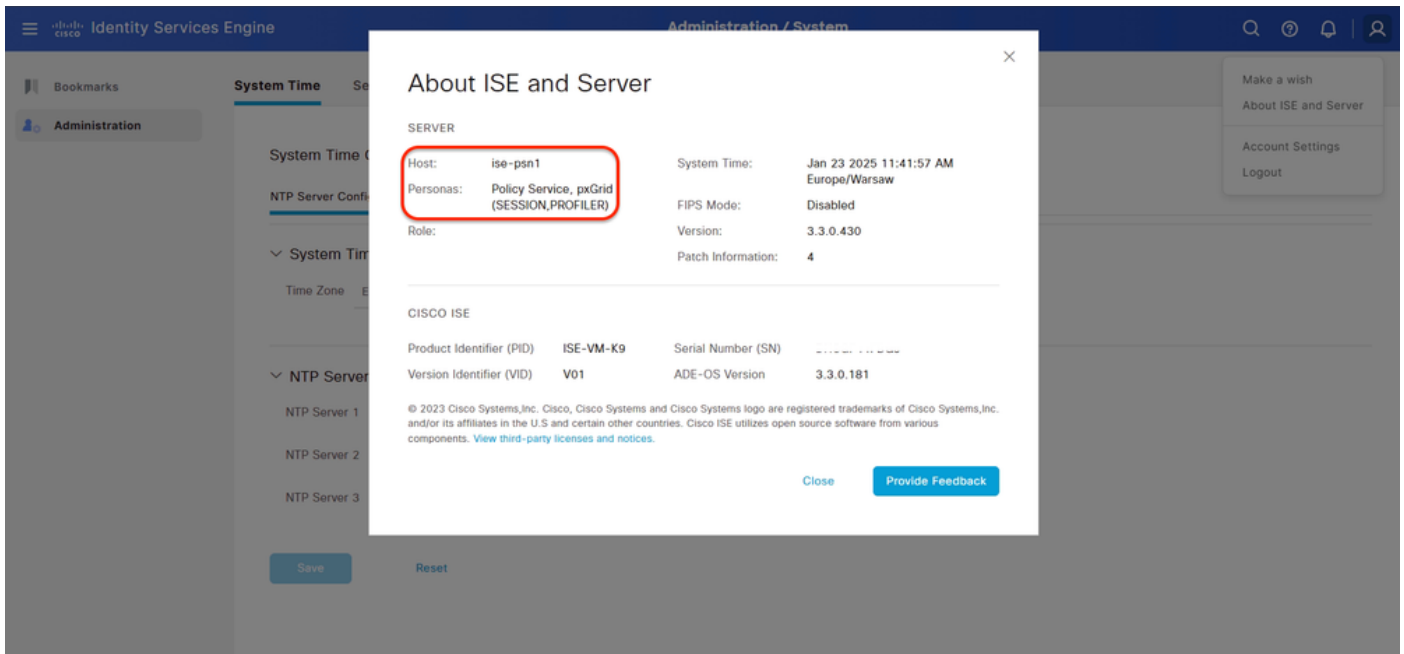
Selected 0 Total 2

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓

(PPAN) Nodi di distribuzione

Passaggio 2. Confermare lo stato del nodo (ise-psn1).

Sfogliare il nodo secondario tramite GUI (<https://ise-psn1.kdlab.local>) e selezionare Login > Informazioni su ISE e server.

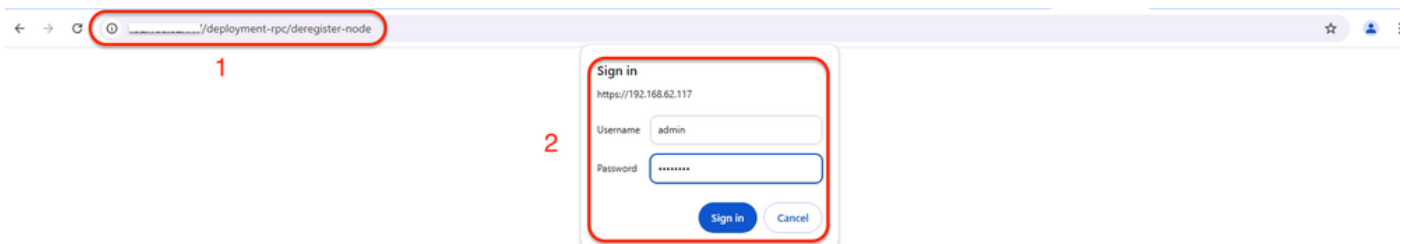


Nodo secondario (ise-psn1) bloccato nello stato della distribuzione distribuita

Soluzione alternativa

Passaggio 1. Annullare la registrazione manuale del nodo (ise-psn1).

Applicare il nodo (ise-psn1) alla distribuzione standalone tramite GUI (<https://<ise-psn1 IP>/deployment-rpc/deregistrator-node>).



Passaggio 2. Verificare (ise-psn1) ora nella distribuzione autonoma.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. A single row is visible for 'ise-psn1' with Role(s) 'STANDALONE' and Node Status 'OK'. The 'ise-psn1' hostname and 'STANDALONE' role are circled in red.

Hostname	Personas	Role(s)	Services	Node Status
ise-psn1	Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER	OK

(ise-psn1) sull'installazione standalone

Passaggio 3. Dopo aver confermato che il nodo è nello stato autonomo, procedere con le stesse operazioni nella sezione Piano d'azione:

1. Rinnovare il certificato di amministratore del nodo (ise-psn1).
2. Registrare il nodo (ise-psn1) nella distribuzione distribuita.
3. Verificare lo stato della distribuzione.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. Three rows are visible: 'ise-ppan', 'ise-psn1', and 'ise-pan'. The 'ise-psn1' row is highlighted with a red circle.

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	OK
ise-psn1	Policy Service, pxGrid		SESSION, PROFILER	OK
ise-pan	Administration, Monitoring	SEC(A), PRI(M)	NONE	OK

(ise-psn1) Aggiunto all'installazione

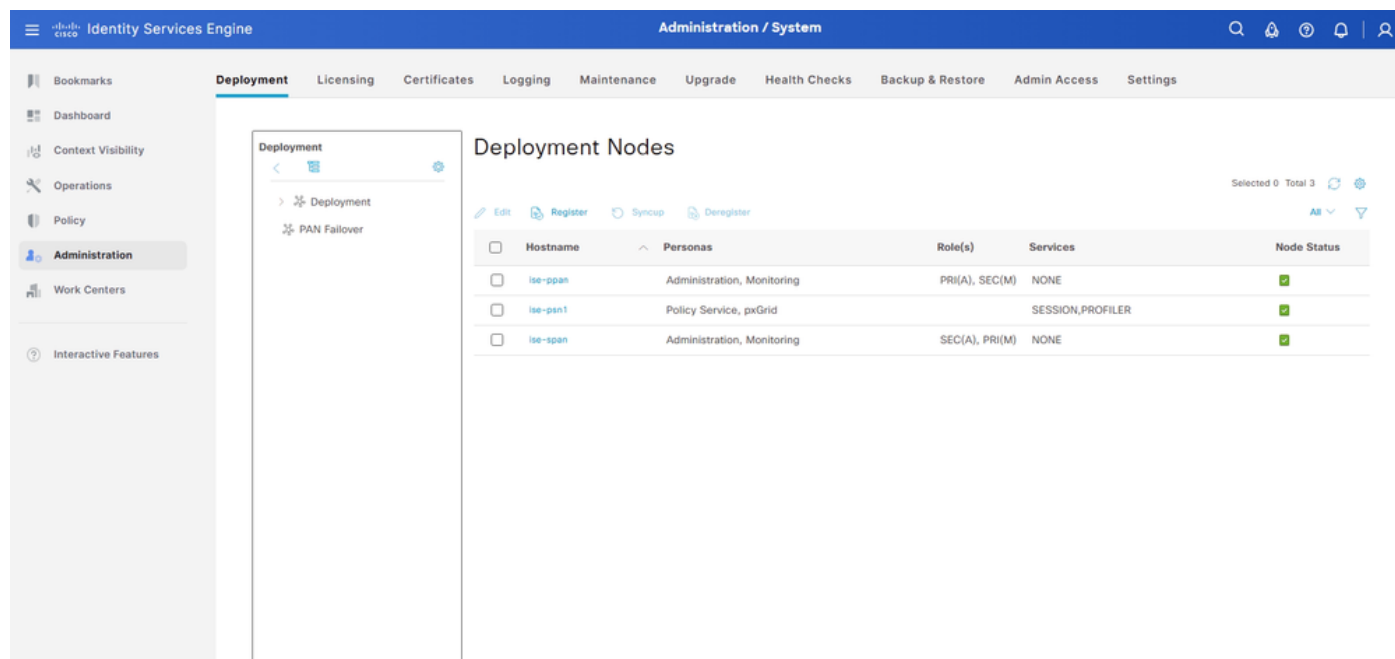
Caso di utilizzo 2: Interfaccia grafica del nodo secondario non registrata non

raggiungibile (ise-psn2)

Convalida lo stato

Passaggio 1. Confermare lo stato della distribuzione distribuita.

Dalla GUI del nodo di amministrazione principale (PPAN). Passare a Amministrazione > Sistema > Distribuzione. È possibile verificare che questo nodo (ise-psn2) sia già stato rimosso dalla registrazione.



(PPAN) Nodi di distribuzione

Passaggio 2. Confermare il (ise-psn2) dello stato del nodo.

A causa del certificato di amministrazione è scaduto in alcuni casi è possibile riscontrare questi sintomi:

- (ise-psn2) GUI non raggiungibile.
- (ise-psn2) CLI (show application status ise) L'applicazione ISE è bloccata (in fase di inizializzazione o non in esecuzione).
- (ise-psn2) CLI (show tech): il nodo è già in fase di distribuzione autonoma.

```
*****
Displaying ISE deployment ...
*****
Node Config Details

NAME                PERSONA          ROLE            ACTIVE          REPLICATION
-----
ise-psn2            PAN,MNT,PSN      STANDALONE      ACTIVE          SYNC COMPLETED
```

(ise-psn2) sull'installazione standalone

Soluzione alternativa

Passaggio 1. Rinnovare il certificato di amministratore del nodo (ise-psn2).

1. Accedere a (ise-psn2) tramite CLI.
2. Immettere application configure ise.
3. Immettere 31 ([31] Generate Self-Signed Admin Certificate).
4. Continuare? y/[n]: y
5. Sostituire il certificato esistente dopo la generazione? y/[n]: y

```
ise-psn2/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
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[39]Reset System 360 Monitoring Page
[40]Enable/Disable Explicit EC Check
[41]Gather Diagnostic data for Certificates
[42]Enable/Disable Parse SAN DirName Extension
[0]Exit

31
After this operation, the ISE node will restart
Do you want to continue? y/[n]: y
Certificate Subject
  *Common Name (CN) : ise-psn2.kdlab2.local
  Enter Organization Unit (OU) : Tech
  Enter Organization (O) : KD
Do you want to replace existing certificate after generation? y/[n]: y
Old Memory Size : 32639004
```


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).