

Integración de ISE 3.3 con Stealthwatch 7.5.1 mediante CA externa

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Configurar](#)

[Sección A: Configuración del certificado de Secure Network Analytics \(Stealthwatch\)](#)

[Parte I - Generación de una CSR para el certificado de cliente pxGrid de Secure Network Analytics](#)

[Parte II - Creación de un certificado de cliente de Secure Network Analytics pxGrid mediante una CA externa](#)

[PARTE III - Adición del certificado de cliente de Secure Network Analytics pxGrid al administrador](#)

[PARTE IV - Importación del certificado raíz de la CA en el almacén de confianza del administrador](#)

[Sección B: Configuración del certificado de Cisco Identity Services Engine 3.3](#)

[PARTE I - Generación de un certificado pxGrid de servidor ISE](#)

[PARTE II - Creación de un certificado pxGrid de servidor ISE mediante una CA externa](#)

[PARTE III: Importación del certificado raíz de la CA en el almacén de confianza de ISE](#)

[PARTE IV: Vincular el certificado ISE a la solicitud de firma de certificado \(CSR\)](#)

[Integrar](#)

[Verificación](#)

[Resolución de problemas](#)

[Problema de resolución de DNS](#)

[Solución](#)

[Error de CA desconocido o falta certificado de confianza](#)

[Solución](#)

[Defectos conocidos](#)

Introducción

Este documento describe los procedimientos para integrar ISE 3.3 con Secure Network Analytics (StealthWatch) mediante conexiones pxGrid.

Prerequisites

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Secure Network Analytics (StealthWatch)
- Certificados TLS/SSL.

- PKI en Windows Server 2016

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 4 de Identity Services Engine (ISE) versión 3.3
- Secure Network Analytics (StealthWatch) 7.5.1
- Windows Server 2016 como servidor de la Autoridad de certificación (CA) externa.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Sección A: Configuración del certificado de Secure Network Analytics (Stealthwatch)

Parte I - Generación de una CSR para el certificado de cliente pxGrid de Secure Network Analytics

1. Inicie sesión en StealthWatch Management Console (SMC).
2. En el menú principal, seleccione Configure > Global > Central Management.



Risk



Monitor



Investigate



Report



Configure

Configure

X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo "Uso mejorado de claves".

6. Descargue un certificado generado en formato Base-64 y guárdelo como pxGrid_client.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

PARTE III - Adición del certificado de cliente de Secure Network Analytics pxGrid al administrador

1. Navegue hasta la sección Identidades de Cliente SSL/TLS adicionales de la Configuración del Administrador en Administración central.
2. La sección Identidades de Cliente SSL/TLS Adicionales contiene un formulario para importar el certificado de cliente creado.
3. Asigne un nombre descriptivo al certificado y haga clic en Seleccionar archivo para localizar el archivo del certificado.
4. Seleccione el archivo CA .cer raíz o emisor o el archivo de cadena de certificados (.pem / .cer / .crt) en la sección Archivo de certificado de cadena.
5. Haga clic en Agregar identidad de cliente para agregar el certificado al sistema.

6. Haga clic en Aplicar configuración para guardar los cambios.

PARTE IV - Importación del certificado raíz de la CA en el almacén de confianza del administrador

1. Navegue hasta la página de inicio del Servicio de certificados de Active Directory de MS y seleccione Descargar un certificado de CA, cadena de certificados o CRL.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:[Request a certificate](#)[View the status of a pending certificate request](#)[Download a CA certificate, certificate chain, or CRL](#)

2. Seleccione el formato Base-64, luego haga clic en Descargar certificado CA.

3. Guarde el certificado como CA_Root.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:**Encoding method:**☐ DER☒ Base 64[Install CA certificate](#)[Download CA certificate](#)[Download CA certificate chain](#)[Download latest base CRL](#)[Download latest delta CRL](#)

4. Inicie sesión en StealthWatch Management Console (SMC).

5. En el menú principal, seleccione Configure > Global > Central Management.

6. En la página Inventario, haga clic en el icono (puntos suspensivos) del jefe.

7. Seleccione Editar Configuración de Dispositivo.

8. Seleccione la pestaña General.

9. Navegue hasta la sección Trust Store e importe el certificado CA_Root.cer exportado anteriormente.

10. Haga clic en Agregar nuevo.

Central Management Inventory Data Store Update Manager App Manager Smart Licensing Database

Inventory / Appliance Configuration

Appliance Configuration - Manager

smcra (10.106.127.50) / Last Updated: 2/8/2025, 5:30:58 PM by admin

Cancel Apply Settings

Configuration Menu

Appliance Network Services **General**

☐ Enable FIPS Encryption Libraries

☐ Enable Common Criteria Encryption Libraries

SMTP Configuration

SMTP Server

Port

From Email

User Name

Password

Encryption Type

☒ SMTPS ☐ STARTTLS ☐ Un-Encrypted

Backup Configuration Encryption

Make sure you save your password. If you lose your password, you can change it. However, you will not be able to restore a backup configuration file without the password.

☐ Enable Encryption

Backup Configuration Password

Confirm Password

External Services

If you enable a service, make sure you enable it on the other required appliances. Refer to the tooltip for requirements.

☒ Enable Cisco Security Cloud Control

☒ Enable Customer Success Metrics

☒ Enable Threat Feed

Feed Confidence Level

7

DoDIN Notifications

☐ Enable

To Email *

Trust Store

Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
yy1nde2owmzmdu5ndc2m2n2mu...ert	Secure Network Analytics	Secure Network Analytics	2024-06-20 20:17:15	2029-06-21 20:17:15	403c0116b1af4d3b71e9060afdb...	4096	Delete
fc751new.www.cisco.com	Secure Network Analytics	Secure Network Analytics	2024-06-23 12:14:09	2029-06-24 12:14:09	14e60739401a8e204c7f03b12279...	4096	Delete
AWS	Amazon	Amazon	2015-05-26 05:30:00	2038-01-17 05:30:00	66c9fcf99bfb0a39e2f0788a43e69...	2048	Delete

5 items per page 1 - 3 of 3 items Page 1 of 1

11. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Seleccionar archivo... para seleccionar el certificado de CA de ISE exportado anteriormente.

12. Haga clic en Agregar certificado para guardar los cambios.

Add Certification Authority Certificate

Friendly Name *

AVASTEROOTCA

Certificate File *

AVASTE_ROOT.cer

Select file...

Cancel Add Certificate

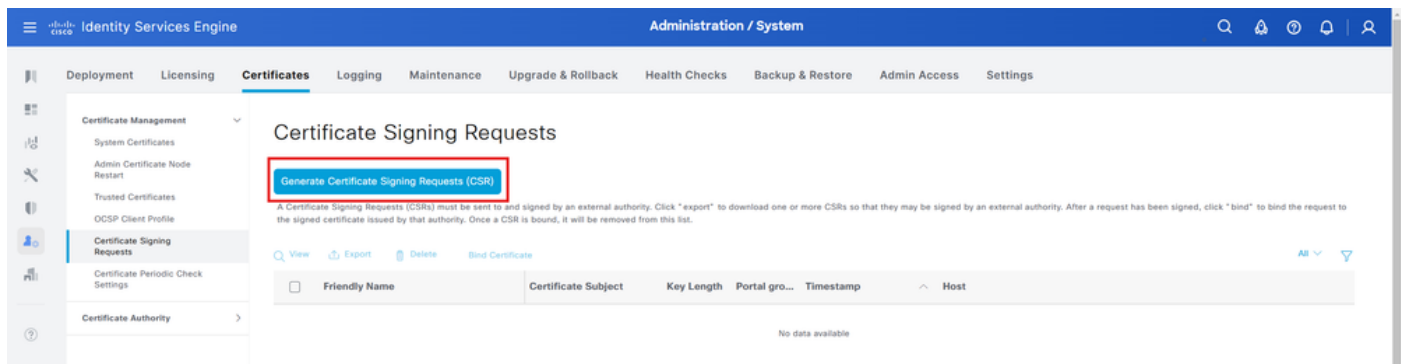
13. Haga clic en Aplicar configuración para guardar los cambios.

Sección B: Configuración del certificado de Cisco Identity Services Engine 3.3

PARTE I - Generación de un certificado ISE Server pxGrid

Generar una CSR para un certificado pxGrid de servidor ISE:

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).
2. Navegue hasta Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificado.
3. Seleccione Generar Solicitud de Firma de Certificado (CSR).



4. Seleccione pxGrid en el campo Certificate(s) is used for.
5. Seleccione el nodo ISE para el que se genera el certificado.
6. Rellene los detalles de otros certificados según sea necesario.
7. Haga clic en Generar.

Usage

Certificate(s) will be used for pxGrid

Allow Wildcard Certificates ☐ ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ avasteise271	avasteise271#pxGrid

Subject

Common Name (CN)
SFQDNS ⓘ

Organizational Unit (OU)
AAA ⓘ

Organization (O)
Cisco ⓘ

City (L)
Bangalore

State (ST)
KA

Country (C)
IN

Subject Alternative Name (SAN)

⋮ DNS Name	avasteise271.avaste.local	— +
⋮ IP Address	10.127.197.128	— + ⓘ

* Key type
RSA ⓘ

* Key Length
4096 ⓘ

* Digest to Sign With
SHA-384

Certificate Policies

Generate Cancel

8. Haga clic en Exportar y Guardar el archivo localmente.

×

Successfully generated CSR(s) ✓

Certificate Signing request(s) generated:

avasteise271#pxGrid

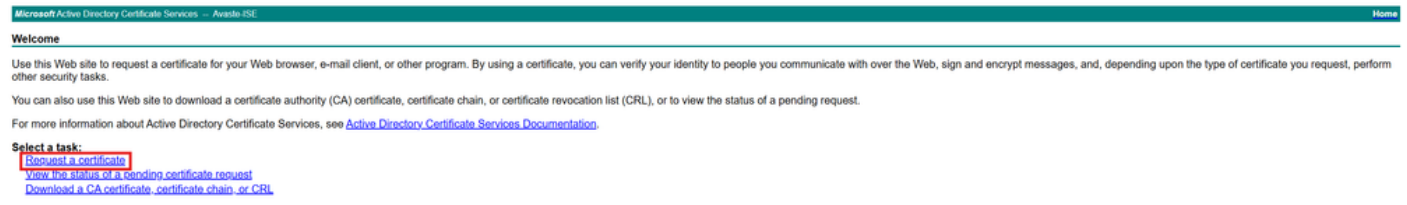
Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK Export

PARTE II - Creación de un certificado pxGrid de servidor ISE mediante una CA externa

1. Navegue hasta Servicio de certificados de Active Directory de MS, <https://server/certsrv/>, donde el servidor es IP o DNS de su servidor MS.

2. Haga clic en Solicitar un certificado.

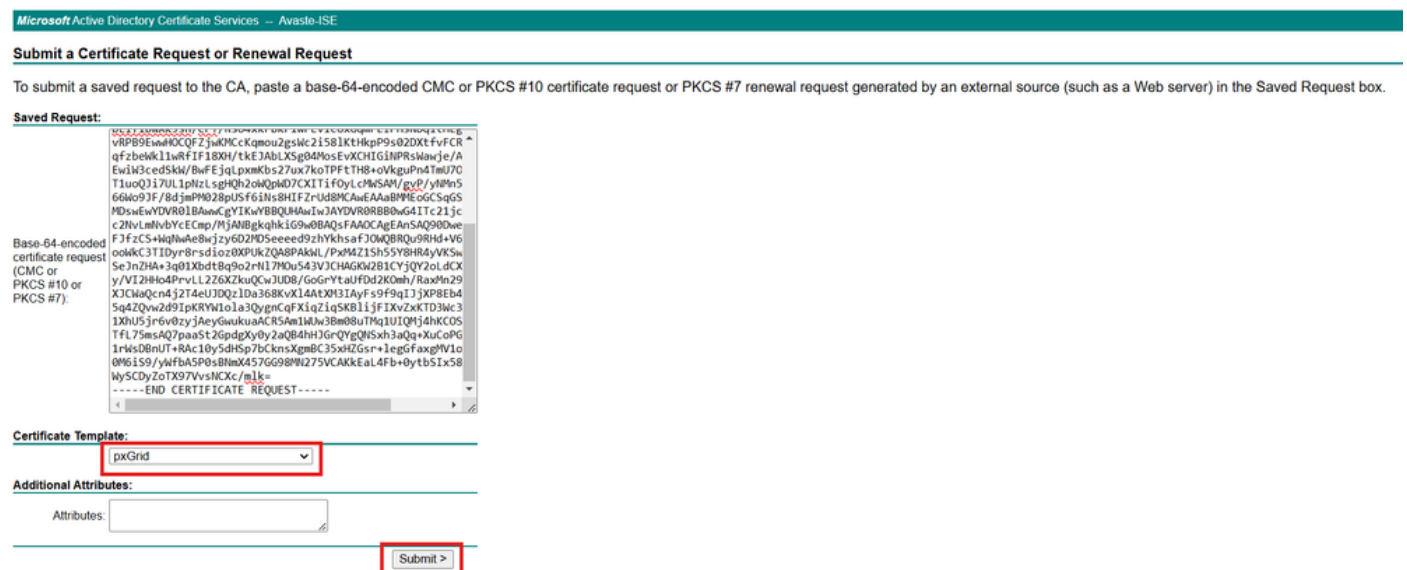


3. Seleccione esta opción para ejecutar una solicitud de certificado avanzada.



4. Copie el contenido del CSR generado en la sección anterior en el campo Solicitud Guardada.

5. Seleccione pxGrid como Plantilla de Certificado y, a continuación, haga clic en Enviar.





Nota: La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo "Uso mejorado de claves".

6. Descargue el certificado generado en formato Base-64 y guárdelo como ISE_pxGrid.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

PARTE III: Importación del certificado raíz de la CA en el almacén de confianza de ISE

1. Navegue hasta la página de inicio del Servicio de certificados de MS Active Directory y seleccione Descargar un certificado de CA, cadena de certificados o CRL.

Microsoft Active Directory Certificate Services -- Avaste-ISE Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

2. Seleccione el formato Base-64, luego haga clic en Descargar certificado CA.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Avaste-ISE] ▲

▼

Encoding method:

☐ DER

☒ Base 64

[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

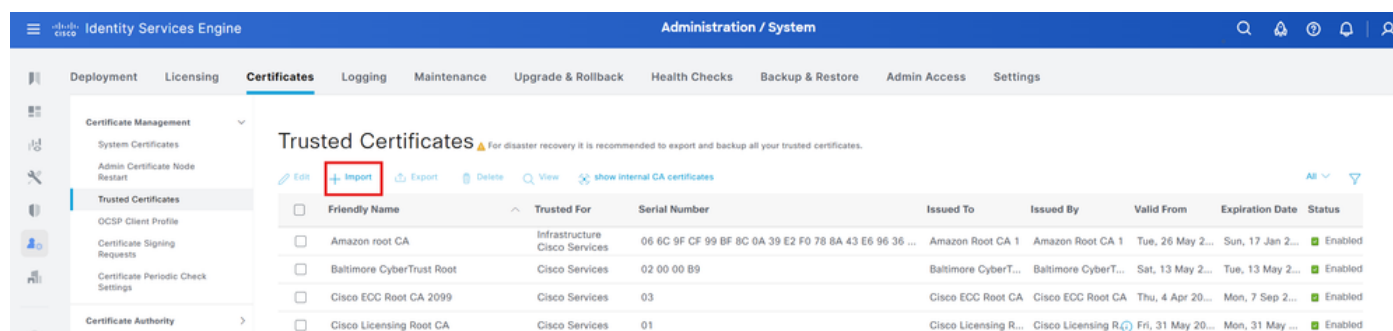
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Guarde el certificado como CA_Root.cer.

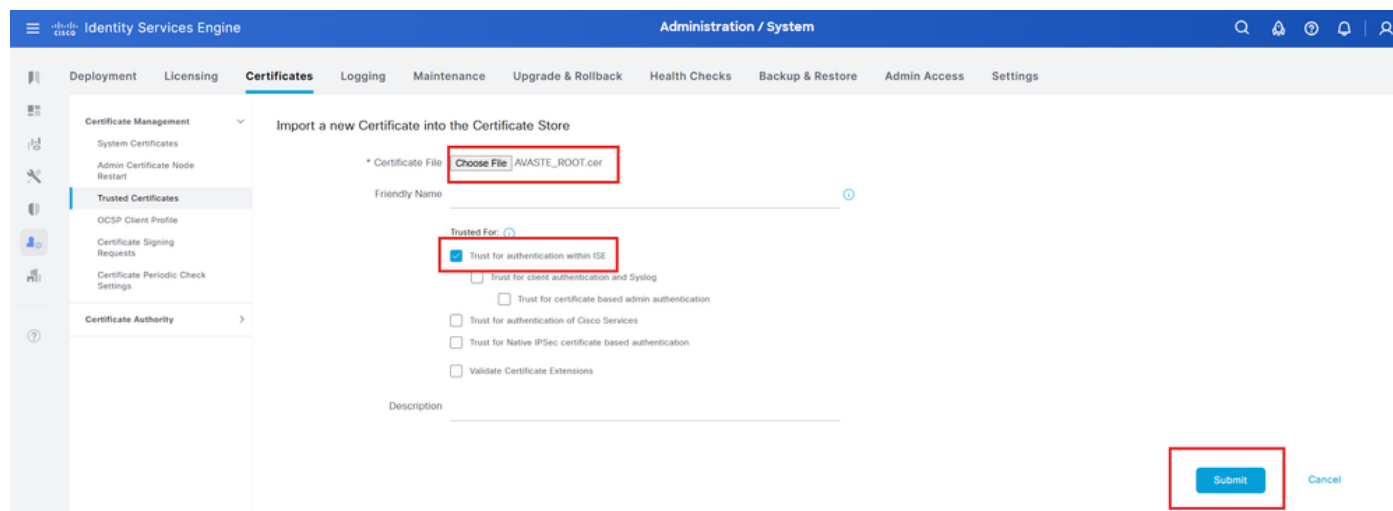
4. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

5. Seleccione Administration > System > Certificates > Certificate Management > Trusted Certificates.



6. Seleccione Importar > Archivo de certificado e Importar el certificado raíz.

7. Asegúrese de que la casilla de verificación Confiar en la autenticación dentro de ISE esté activada.



8. Haga clic en Enviar.

PARTE IV: Vincular el certificado ISE a la solicitud de firma de certificado (CSR)

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

2. Seleccione Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificado.

3. Seleccione el CSR generado en la sección anterior y, a continuación, haga clic en Enlazar certificado.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback 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 Settings
- Certificate Authority

Certificate Signing Requests

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Requests (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, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

[View](#) [Export](#) [Delete](#) [Bind Certificate](#)

☐	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☒	avasteise271pxGrid	CN=avasteise271.avaste...	4096		Sat, 8 Feb 2025	avasteise271

4. En el formulario de certificado firmado de CA de enlace, seleccione el certificado ISE_pxGrid.cer generado anteriormente.

5. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Enviar.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback 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 Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File [Choose File](#) ISE_pxgrid.cer.cer

Friendly Name ISE-pxGRID

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

[Submit](#) [Cancel](#)

7. Haga clic en Sí si el sistema le solicita que sustituya el certificado.

8. Seleccione Administration > System > Certificates > System Certificates.

9. Puede ver el certificado pxGrid creado firmado por la CA externa en la lista.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback 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 Settings
- Certificate Authority

System Certificates

[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

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

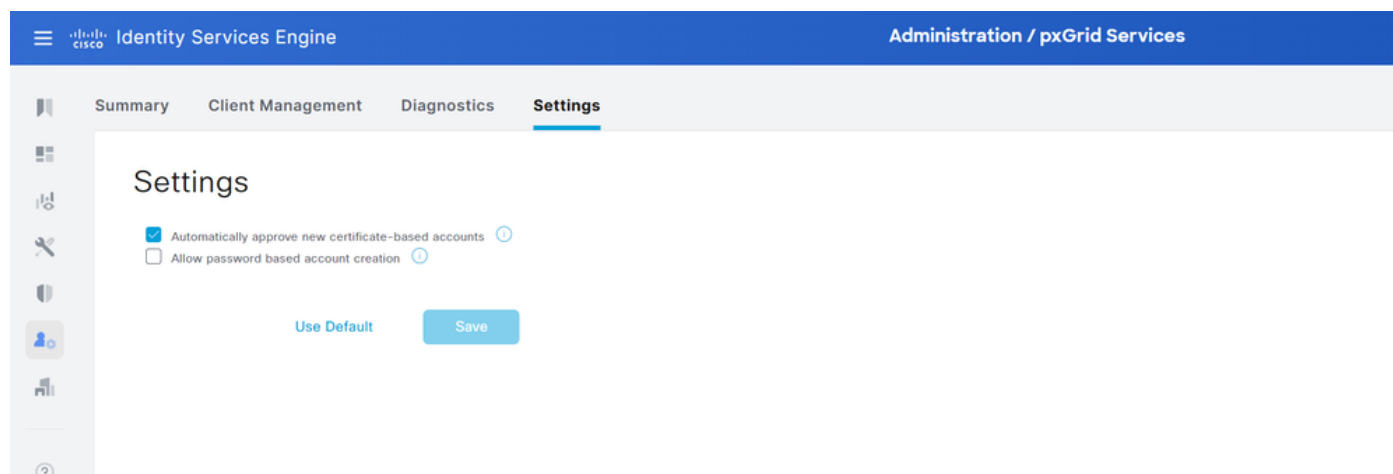
☐	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
☒	avasteise271							
☐	CN=avasteise271.avaste.local, OU=Certificate Services System Certificate, Endpoint Sub CA - avasteise271800002	Not in use		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	Default self-signed server certificate	RADIUS DTLS		avasteise271.avaste.local	avasteise271.avaste.local	Fri, 16 Aug 2024	Tue, 2 Oct 2029	Active
☐	Default self-signed saml server certificate - CN=SAML_avasteise271.avaste.local	SAML		SAML_avasteise271.avaste.local	SAML_avasteise271.avaste.local	Fri, 16 Aug 2024	Wed, 15 Aug 2029	Active
☐	CN=avasteise271.avaste.local, OU=ISE Messaging Service Certificate Services Endpoint Sub CA - avasteise271800003	ISE Messaging Service		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☒	ISE-pxGRID	pxGrid		avasteise271.avaste.local	Avaste-ISE	Sat, 8 Feb 2025	Mon, 8 Feb 2027	Active
☐	AWASTE-2024	Admin, Portal, EAP Authentication	Default Portal Certificate Group	avasteise271.avaste.local	Avaste-ISE	Sun, 25 Aug 2024	Tue, 25 Aug 2026	Active

Los certificados ya están implementados. Continúe con la integración.

Integrar

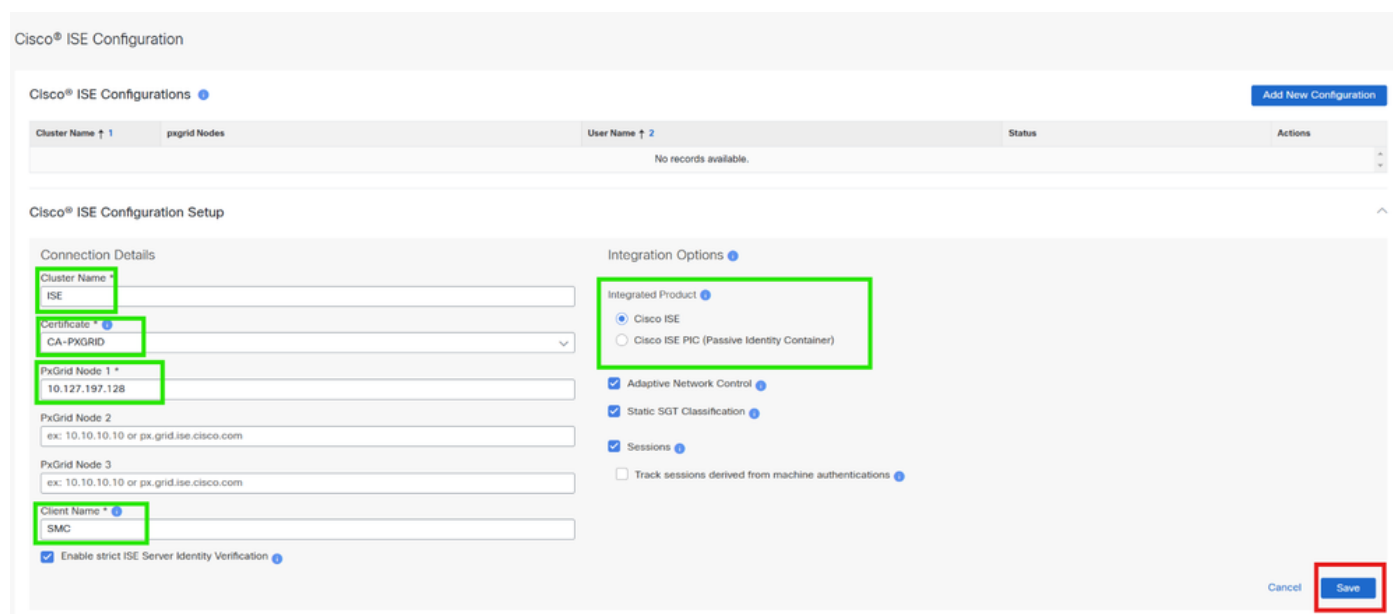
Antes de proceder a la integración, asegúrese de que:

Para Cisco ISE, en Administration > pxGrid Services > Settings y Check Apruebe automáticamente las nuevas cuentas basadas en certificados para que la solicitud del cliente se apruebe automáticamente y se guarde.



En StealthWatch Management Console (SMC), Para abrir la página de configuración de ISE:

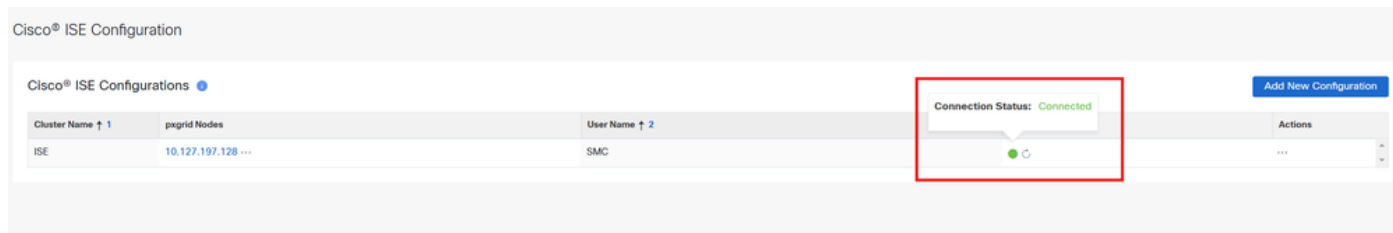
1. Seleccione Configurar > Integraciones > Cisco ISE.
2. En la esquina superior derecha de la página, haga clic en Agregar nueva configuración.
3. Introduzca el nombre del cluster, seleccione el certificado & Integration Product, el nodo pxGrid IP y haga clic en Save.



Verificación

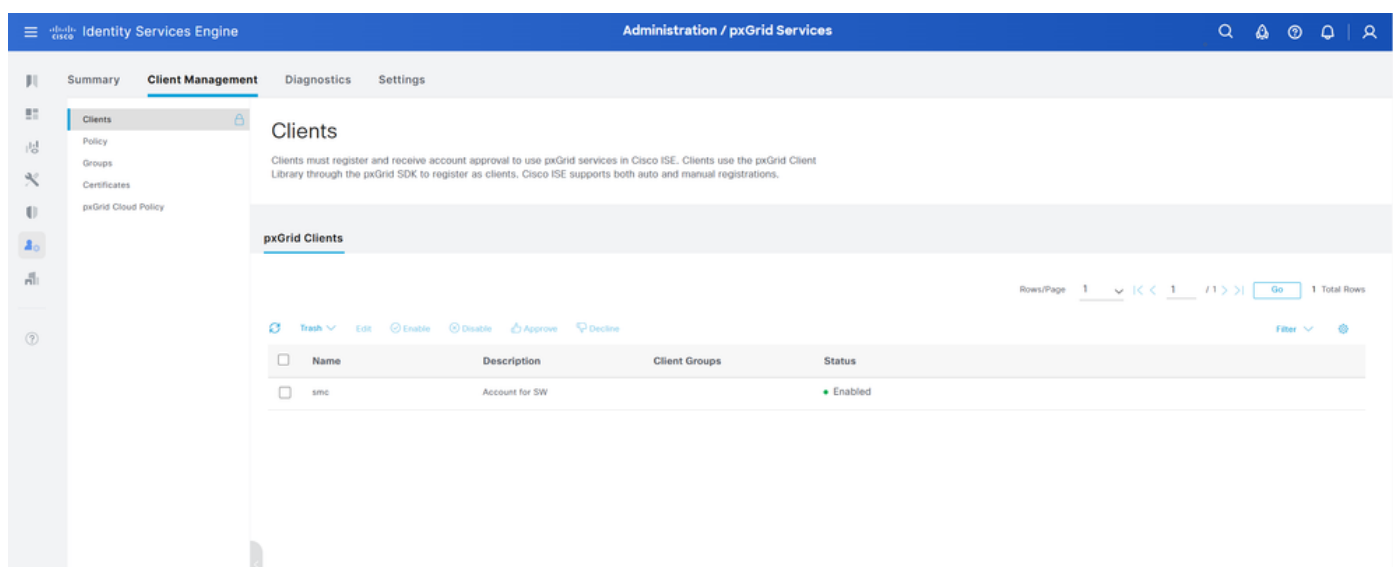
Actualice la página de configuración de ISE en StealthWatch Management Console (SMC).

1. Vuelva a la página de configuración de ISE en la aplicación web y actualice la página.
2. Confirme que el indicador de estado del nodo situado junto al campo Dirección IP aplicable es Verde, lo que indica que se ha establecido una conexión con el clúster ISE o ISE-PIC.



En Cisco ISE, navegue hasta Administration > pxGrid Services > Client Management > Clients.

Esto genera el SMC como un cliente pxgrid con el estado Enabled.



Para verificar la suscripción a los temas en Cisco ISE, navegue hasta Administration > pxGrid Services > Diagnostics > Websocket > Topics

Esto genera un SMC suscrito a estos temas.

tema SGT de Trustsec

▼ /topic/com.cisco.ise.config.trustsec.security.group	0	1
---	---	---

Rows/Page
10
▼
|<<
1
/ 1 >>|
Go
1 Total Rows

Connection Name	Messaging Role
SMC	Sub

tema de directorio de sesión de ISE

▼ /topic/com.cisco.ise.session	1	1
--------------------------------	---	---

Rows/Page
10
▼
|<<
1
/ 1 >>|
Go
2 Total Rows

Connection Name	Messaging Role
~ise-mnt-avasteise271	Pub
SMC	Sub

tema Enlaces de ISE SXP

▼ /topic/com.cisco.ise.sxp.binding	0	1
------------------------------------	---	---

Rows/Page
10
▼
|<<
1
/ 1 >>|
Go
1 Total Rows

Connection Name	Messaging Role
SMC	Sub

Cisco ISE Pxgrid-server.log en el nivel TRACE.

2025-02-08 18:07:11,086 TRACE [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,110 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::

```

2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,112 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::
2025-02-08 18:07:11,321 DEBUG [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib

]
2025-02-08 18:07:11,322 DEBUG [pxgrid-http-pool20][[]] cisco.cpm.pxgridwebapp.config.AuthzEvaluator -:::
2025-02-08 18:07:11,322 INFO [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint

] session=[id=8,client=SMC,server=wss://avasteise271.avaste.local:8910/pxgrid/ise/pubsub]
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::
2025-02-08 18:07:11,323 TRACE [WsIseClientConnection-1010][[]] cpm.pxgrid.ws.client.WsEndpoint -:::
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib

]
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib

]
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistrib
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

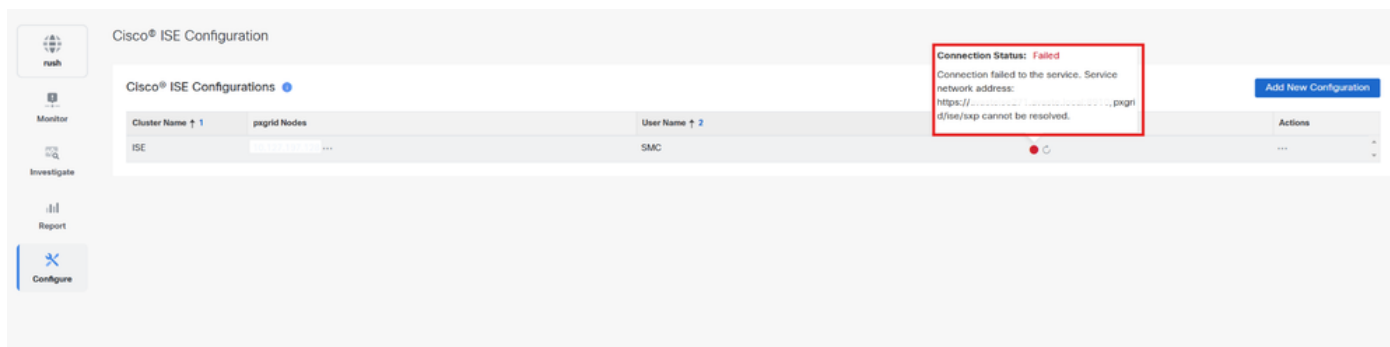
] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```

Resolución de problemas

Problema de resolución de DNS

Esto produce un mensaje de error como "Connection Status; Error de conexión al servicio. Dirección de red del servicio:
<https://isehostnameeme.domain.com:891pxgridiisessxpxp> no se puede resolver":



Solución

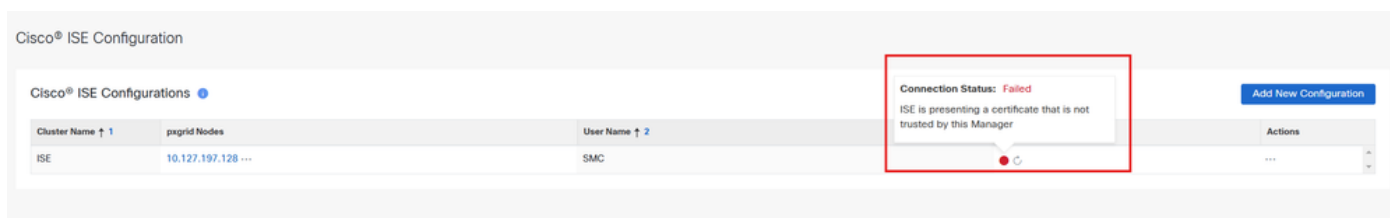
Idealmente, esto debe solucionarse en el servidor DNS para las búsquedas directas e inversas de este FQDN de ISE. Sin embargo, se puede agregar una solución temporal para la resolución local:

1. Inicie sesión en StealthWatch Management Console (SMC).
2. En el menú principal, seleccione Configure > Global > Central Management.
3. En la página Inventario, haga clic en el icono (Puntos suspensivos) del jefe.
4. Seleccione Editar Configuración del Dispositivo.
5. Servicios de red y agregue una entrada de resolución local para este FQDN de ISE.



Error de CA desconocido o falta certificado de confianza

Esto produce un mensaje de error como "ISE está presentando un certificado que no es de confianza para este administrador":



Se puede ver una referencia de registro similar en el archivo oSMCMsvcvise-client.log. Ruta: catlancopepe/var/logs/containsvcvise-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLException
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:395)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:2065)
```

```

snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClient
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:2
snasmc1 docker/svc-ise-client[1453]: at java.base/java.lang.Thread.run(Thread.java:829)
snasmc1 docker/svc-ise-client[1453]: Caused by: javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFatal
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jsse.provider.ProvSSLEngine.unwrap(ProvSSLEngi
snasmc1 docker/svc-ise-client[1453]: at java.base/javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.jav
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(S
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpC
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFill
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnection
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(Selectable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThre
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(Queue
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.

```

Solución

1. Inicie sesión en StealthWatch Management Console (SMC).
2. En el menú principal, seleccione Configure > Global > Central Management.
3. En la página Inventario, haga clic en el icono (puntos suspensivos) del jefe.
4. Seleccione Editar Configuración del Dispositivo.
5. Seleccione la pestaña General.
6. Navegue hasta la sección Almacén de confianza y asegúrese de que el emisor del certificado Pxgrid de Cisco ISE forme parte del almacén de confianza.

Defectos conocidos

ID de la falla	Descripción
ID de bug de Cisco 18119	ISE está seleccionando un paquete de saludo del servidor Cipher ITLS no compatible
ID de bug de Cisco 01634	No se pueden poner en cuarentena los dispositivos mediante la condición EPS

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).