

Configuración de la autenticación EAP-TLS con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Obtener certificados de servidor y cliente](#)

[Paso 1. Generar una solicitud de firma de certificado desde ISE](#)

[Paso 2. Importar certificados de CA a ISE](#)

[Paso 3. Obtener certificado de cliente para terminal](#)

[Dispositivos de red](#)

[Paso 4. Agregar el dispositivo de acceso a la red en ISE](#)

[Elementos de política](#)

[Paso 5. Utilizar origen de identidad externo](#)

[Paso 6. Crear el perfil de autenticación de certificado](#)

[Paso 7. Agregar a una secuencia de origen de identidad](#)

[Paso 8. Definir el servicio de protocolos permitidos](#)

[Paso 9. Crear el perfil de autorización](#)

[Políticas de seguridad](#)

[Paso 10. Crear el conjunto de políticas](#)

[Paso 11. Crear una política de autenticación](#)

[Paso 12. Crear la directiva de autorización](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas comunes y técnicas para solucionar problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración inicial para introducir el protocolo de autenticación extensible-autenticación de seguridad de capa de transporte con Cisco ISE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del flujo de comunicaciones EAP y RADIUS.
- Conocimiento básico de la autenticación RADIUS con métodos de autenticación basados en certificados en términos del flujo de comunicación.
- Comprensión de las diferencias entre Dot1x y MAC Authentication Bypass (MAB).
- Comprensión básica de la infraestructura de clave pública (PKI).
- Familiaridad con la forma de obtener certificados firmados de una entidad emisora de certificados

- (CA) y administrar certificados en los terminales.
- Configuración de los parámetros relacionados con la autenticación, autorización y administración de cuentas (AAA) (RADIUS) en un dispositivo de red (con cables o inalámbrico).
- Configuración del suplicante (en el terminal) para su uso con RADIUS/802.1x.

Componentes Utilizados

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

- Identity Services Engine (ISE) versión 3.x.
- CA: para emitir certificados (puede ser una CA empresarial, una CA pública o de terceros, o utilizar el [portal de aprovisionamiento de certificados](#)).
- Active Directory (origen de identidad externo): desde Windows Server; donde [es compatible con ISE](#).
- Dispositivo de acceso a la red (NAD): puede ser switch (con cables) o [controlador de LAN inalámbrica \(WLC\)](#) (inalámbrico) configurado para 802.1x/AAA.
- Terminal: certificados emitidos para la identidad (de usuario) y la configuración del solicitante que se pueden autenticar para el acceso a la red a través de RADIUS/802.1x: autenticación de usuario. Es posible obtener un certificado de equipo, pero no se utiliza en este ejemplo.

Nota: puesto que esta guía utiliza ISE Release 3.1, todas las referencias de documentación se basan en esta versión. Sin embargo, es posible realizar una configuración idéntica o similar y es totalmente compatible con versiones anteriores de Cisco ISE.

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.

Antecedentes

El objetivo principal es la configuración de ISE, que se puede aplicar a varios escenarios, como la autenticación (aunque sin limitarse a ella) con un teléfono/terminal IP conectado a través de redes por cable o inalámbricas.

Para el alcance de esta guía, es importante comprender estas fases del flujo de autenticación de ISE (RADIUS):

- Autenticación: identifica y valida la identidad final (equipo, usuario, etc.) que solicita acceso a la red.
- Autorización: determine qué permisos/acceso se pueden otorgar a la identidad final en la red.
- Contabilidad: informe y realice un seguimiento de la actividad de la red de la identidad final una vez que se haya logrado el acceso a la red.

Configurar

Obtener certificados de servidor y cliente

Paso 1. Generar una solicitud de firma de certificado desde ISE

El primer paso consiste en generar una solicitud de firma de certificado (CSR) a partir de ISE y enviarla a la

CA (servidor) para obtener el certificado firmado emitido a ISE, como certificado del sistema. ISE puede presentar este certificado como un certificado de servidor durante la autenticación EAP-TLS (protocolo de autenticación extensible-autenticación de seguridad de capa de transporte). Esto se realiza en la interfaz de usuario de ISE. Desplácese hasta **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**. Debajo **Certificate Signing Requests**, haga clic en **Generate Certificate Signing Requests (CSR)** como se muestra en esta imagen.

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) 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 that authority. Once a CSR is bound, it will be removed from this list.

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

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	^
No data available						

Los tipos de certificado requieren diferentes usos de clave extendida. Esta lista describe qué usos de clave extendidos se requieren para cada tipo de certificado:

Certificados de identidad ISE

- Varios usos (Admin, EAP, Portal, pxGrid): autenticación de cliente y servidor
- Admin - Autenticación del servidor
- Autenticación EAP - Autenticación del servidor
- Autenticación de seguridad de la capa de transporte del datagrama (DTLS) - Autenticación del servidor
- Portal - Autenticación del servidor
- pxGrid - Autenticación de cliente y servidor
- Lenguaje de marcado de aserción de seguridad (SAML): certificado de firma SAML
- Servicio de mensajería ISE: genere un certificado de firma o genere un certificado de mensajería completamente nuevo

De forma predeterminada, el certificado del sistema de servicio de mensajería de ISE es para la replicación de datos en todos los nodos ISE de la implementación, el registro de nodos y otras comunicaciones entre nodos, y está presente y lo emite el servidor de la autoridad de certificación interna (CA) de ISE (interno de ISE). No se requiere ninguna acción para completar con este certificado.

El certificado del sistema de administración se utiliza para identificar cada nodo de ISE, por ejemplo, cuando se utiliza la API asociada a la interfaz de usuario de administración (administración) y para algunas comunicaciones entre nodos. Para configurar ISE por primera vez, establezca el certificado del sistema de administración. Esta acción no está directamente relacionada con esta guía de configuración.

Para realizar IEEE 802.1x a través de EAP-TLS (autenticación basada en certificados), realice la acción para el certificado del sistema de autenticación EAP, ya que se utiliza como el certificado de servidor presentado al terminal/cliente durante el flujo EAP-TLS; como resultado, se protege dentro del túnel TLS. Para comenzar, cree un CSR para crear el certificado del sistema de autenticación EAP y entréguelo al personal que administra los servidores de CA de su organización (o al proveedor de CA pública) para su firma. El resultado final es el certificado firmado por la CA que se enlaza a CSR y se asocia a ISE con estos pasos.

En el formulario de Solicitud de firma de certificado (CSR), elija estas opciones para completar el CSR y obtener su contenido:

- Uso del certificado, para este ejemplo de configuración, elija **EAP Authentication**.
- Si piensa utilizar una declaración comodín en el certificado, ***.example.com**, también debe comprobar el **Allow Wildcard Certificate** casilla de verificación. La mejor ubicación es el campo de certificado Nombre alternativo del sujeto (SAN) para comprobar la compatibilidad con cualquier uso y entre varios tipos diferentes de sistemas operativos de terminales que pueden estar presentes en el entorno.
- Si no ha elegido colocar una sentencia de comodín en el certificado, elija a qué nodos ISE desea asociar el certificado firmado por la CA (después de la firma).

Nota: cuando enlaza el certificado firmado por la CA que contiene la sentencia de comodín a varios nodos dentro de la CSR, el certificado se distribuye a cada nodo de ISE (o a los nodos seleccionados) en la implementación de ISE y los servicios se pueden reiniciar. Sin embargo, el reinicio de los servicios se limita automáticamente a un nodo cada vez. Supervise el reinicio de los servicios a través del `show application status ise ISE CLI`.

A continuación, debe completar el formulario para definir el asunto. Esto incluye los campos de certificado Nombre común (CN), Unidad organizativa (OU), Organización (O), Ciudad (L), Estado (ST) y País (C). La variable `$FQDN$` es el valor que representa el nombre de dominio completamente calificado de administración (nombre de host + nombre de dominio) asociado con cada nodo de ISE.

- Subject Alternative Name (SAN) También deben rellenarse los campos para incluir la información necesaria y deseada que se utilizará para establecer la confianza. Como requisito, debe definir la entrada DNS que apunta al FQDN de los nodos ISE asociados a este certificado, una vez firmado el certificado.
- Por último, asegúrese de definir el tipo de clave, la longitud de la clave y el resumen para firmar adecuados que se ajusten a las capacidades de los servidores de la CA y tengan en cuenta las buenas prácticas de seguridad. Los valores predeterminados son: RSA, 4096 bits y SHA-384, respectivamente. Las opciones disponibles y la compatibilidad se muestran en esta página en la interfaz de usuario de administración de ISE.

Este es un ejemplo de un formulario CSR completado sin utilizar una instrucción comodín. Asegúrese de utilizar valores reales específicos del entorno:

Usage

Certificate(s) will be used for EAP Authentication ▼

Allow Wildcard Certificates ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise	ise#EAP Authentication
<input checked="" type="checkbox"/> ise2	ise2#EAP Authentication
<input checked="" type="checkbox"/> ise3	ise3#EAP Authentication

Subject

Common Name (CN)
\$FQDN\$ ⓘ

Organizational Unit (OU)
 ⓘ

Organization (O)
Example Company ⓘ

City (L)
San Jose

State (ST)
California

Country (C)
US

Subject Alternative Name (SAN)

⋮	DNS Name	▼	ise.example.com	-	+	
⋮	DNS Name	▼	ise2.example.com	-	+	
⋮	DNS Name	▼	ise3.example.com	-	+	ⓘ

* Key type

RSA ▼ ⓘ

* Key Length

4096 ▼ ⓘ

* Digest to Sign With

SHA-384 ▼

Certificate Policies

Ejemplo de CSR

Para guardar el CSR, haga clic en **Generate**. Haga clic en **Export**, situado en la parte inferior derecha, para exportar los archivos CSR desde este mensaje:

×

Successfully generated CSR(s)

Certificate Signing request(s) generated:

ise#EAP Authentication
ise2#EAP Authentication
ise3#EAP Authentication

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

OK Export

Ejemplo de Exportar CSR

Puede encontrar más información sobre los certificados para su uso con ISE en la Guía del administrador de Cisco Identity Services Engine, versión 3.1 > capítulo: Basic Setup > [Certificate Management in Cisco ISE](#) e [Install a Third-Party CA-Signed Certificate in ISE](#).

Paso 2. Importar certificados de CA a ISE

Una vez que la CA devuelve el certificado firmado, también incluye la cadena completa de la CA compuesta por un certificado raíz y uno o varios certificados intermedios. La interfaz de usuario de administración de ISE le obliga a importar todos los certificados de la cadena de CA en primer lugar, antes de la asociación o carga de cualquier certificado del sistema. Esto se realiza para garantizar que cada certificado del sistema esté asociado correctamente con la cadena de CA (también conocida como certificado de confianza) dentro del software de ISE.

Estos pasos son la mejor manera de importar los certificados de CA y el certificado del sistema en ISE:

1. Para importar el certificado raíz en la GUI de ISE, vaya a **Administration > System: Certificates > Certificate Management**. Debajo **Trusted Certificates**, haga clic en **Import** y marque las casillas de verificación **Confianza para autenticación dentro de ISE** (Infraestructura) y **Confianza para autenticación de cliente y Syslog** (Terminales).

Usage

Trusted For: ⓘ

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services

Uso de certificados para la cadena de CA

2. Repita el paso anterior para cada certificado intermedio como parte de la cadena de certificados de la CA.
3. Una vez que todos los certificados, como parte de la cadena completa de CA, se hayan importado al almacén de certificados de confianza de ISE, vuelva a la GUI de ISE y navegue hasta **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Busque la entrada CSR en **Nombre descriptivo** que corresponda al certificado firmado, haga clic en la casilla de verificación del certificado y, a continuación, haga clic en **Bind Certificate**.

Certificate Signing Requests

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

A Certificate Signing Requests (CSRs) 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 that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete **Bind Certificate** 2)

<input type="checkbox"/>	Friendly Name 1)	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise. example.com ,O=E...	4096		Tue, 10 May 2022	ise
<input type="checkbox"/>	ise2#EAP Authentication	CN=ise2. example.com ,O=...	4096		Tue, 10 May 2022	ise2
<input type="checkbox"/>	ise3#EAP Authentication	CN=ise3. example.com ,O=...	4096		Tue, 10 May 2022	ise3

Enlazar certificado a CSR

Nota: debe vincular un solo certificado firmado por la CA a cada CSR de uno en uno. Repita este procedimiento para los CSR restantes creados para otros nodos ISE de la implementación.

En la página siguiente, haga clic en **Browse** y elija el archivo de certificado firmado, defina el nombre descriptivo que desee y elija los usos del certificado. Enviar para guardar los cambios.

Bind CA Signed Certificate

* Certificate File

EXAMPLE_ISE.cer

Friendly Name

EAP Authentication System Certificate ⓘ

Validate Certificate Extensions

ⓘ

y asignarlo al mismo nodo para el que se creó CSR. Repita el mismo proceso para otros nodos u otros usos de certificados.

Paso 3. Obtener certificado de cliente para terminal

Se requiere navegar a través de un proceso similar en el extremo para la creación de un certificado de cliente para su uso con EAP-TLS. Para este ejemplo, necesita un certificado de cliente firmado y emitido para la cuenta de usuario para realizar la autenticación de usuario con ISE. Puede encontrar un ejemplo de cómo obtener un certificado de cliente para el extremo de un entorno de Active Directory en: [Comprensión y configuración de EAP-TLS mediante WLC e ISE > Configurar > Cliente para EAP-TLS](#).

Debido a los múltiples tipos de terminales y sistemas operativos, ya que el proceso puede ser algo diferente, no se proporcionan ejemplos adicionales. Sin embargo, el proceso general es conceptualmente el mismo. Generar una CSR que tenga toda la información relevante que se incluirá en el certificado y que esté firmada por la CA, ya sea un servidor interno del entorno o una empresa pública o de terceros que proporcione este tipo de servicio.

Además, los campos de certificado Nombre común (CN) y Nombre alternativo del sujeto (SAN) incluyen la identidad que se debe utilizar durante el flujo de autenticación. Esto también determina cómo se debe configurar el solicitante para EAP-TLS en términos de identidad: autenticación de equipo y/o usuario, autenticación de equipo o autenticación de usuario. En este ejemplo sólo se utiliza la autenticación de usuario en el resto de este documento.

Dispositivos de red

Paso 4. Agregar el dispositivo de acceso a la red en ISE

El dispositivo de acceso a la red (NAD) al que está conectado un terminal también se configura en ISE para que pueda tener lugar la comunicación RADIUS/TACACS+ (administrador de dispositivos). Entre NAD e ISE, se utiliza un secreto o una contraseña compartidos con fines de confianza.

Para agregar un NAD a través de la GUI de ISE, navegue hasta **Administration > Network Resources: Network Devices > Network Devices** y haga clic en **Add**, que se muestra en esta imagen.

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | Location Services

Network Devices List > Switch

Network Devices

* Name:

Description:

IP Address: /

* Device Profile:

Model Name:

Software Version:

* Network Device Group

Device Type:

IPSEC:

Location:

Ejemplo de Configuración de Dispositivo de Red

Para su uso con la generación de perfiles de ISE, también debe configurar SNMPv2c o SNMPv3 (más seguro) para permitir que el nodo de servicios de políticas de ISE (PSN) se ponga en contacto con el NAD a través de consultas SNMP relacionadas con la autenticación del terminal en ISE con el fin de recopilar atributos para tomar decisiones precisas sobre el tipo de terminal que se utiliza. El siguiente ejemplo muestra cómo configurar SNMP (v2c), desde la misma página que en el ejemplo anterior:

SNMP Settings

* SNMP Version:

* SNMP RO Community:

SNMP Username:

: La misma acción se aplica para agregar grupos de seguridad a una instancia LDAP. En la GUI de ISE, seleccione **Administration > Identity Management: External Identity Sources > LDAP > LDAP instance name > tab: Groups > Add > Select Groups From Directory**.

Paso 6. Crear el perfil de autenticación de certificado

El propósito del perfil de autenticación de certificados es informar a ISE sobre qué campo de certificado se puede encontrar la identidad (equipo o usuario) en el certificado de cliente (certificado de identidad final) presentado a ISE durante EAP-TLS (también durante otros métodos de autenticación basados en certificados). Esta configuración está vinculada a la directiva de autenticación para autenticar la identidad. En la GUI de ISE, vaya a **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** y haga clic en **Add**.

Usar identidad de se utiliza para elegir el atributo de certificado del que se puede encontrar un campo específico para la identidad. Las opciones son:

- Subject - Common Name
- Subject Alternative Name
- Subject - Serial Number
- Subject
- Subject Alternative Name - Other Name
- Subject Alternative Name - EMail
- Subject Alternative Name - DNS

Si el almacén de identidad debe apuntar a Active Directory o LDAP (origen de identidad externo), se puede utilizar una característica denominada [Comparación binaria](#). Binary Comparison realiza una búsqueda de la identidad en Active Directory obtenida del certificado de cliente de la selección **Use Identity From**, que se produce durante la fase de autenticación de ISE. Sin la comparación binaria, la identidad simplemente se obtiene del certificado del cliente y no se busca en Active Directory hasta la fase de autorización de ISE, cuando se utiliza un grupo externo de Active Directory como condición, o cualquier otra condición que se deba realizar externamente a ISE. Para utilizar la comparación binaria, en el **Almacén de identidades** elija el origen de identidad externo (Active Directory o LDAP) donde se puede encontrar la cuenta de identidad final.

Éste es un ejemplo de configuración cuando la identidad se encuentra en el campo Common Name (CN) del certificado de cliente, con la opción Binary Comparison habilitada (opcional):

External Identity Sources

- Certificate Authentication F
- Active Directory
 - AD1
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login

Certificate Authentication Profiles List > Certificate_Profile

Certificate Authentication Profile

* Name: Certificate_Profile

Description: [Empty text area]

Identity Store: All_AD_Join_Points

Use Identity From:

- Certificate Attribute: Subject - Common Name
- Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate in Identity Store:

- Never
- Only to resolve identity ambiguity
- Always perform binary comparison

Perfil de autenticación de certificado

Puede encontrar más información en la Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Configuración básica > Servicio de CA de Cisco ISE > Configurar Cisco ISE para utilizar certificados para autenticar dispositivos personales > [Crear un perfil de autenticación de certificado para la autenticación basada en TLS.](#)

Paso 7. Agregar a una secuencia de origen de identidad

La secuencia de origen de identidad se puede crear desde la GUI de ISE. Desplácese hasta **Administration > Identity Management**. Debajo **Identity Source Sequences**, haga clic en **Add**.

El siguiente paso es agregar el perfil de autenticación de certificado a una secuencia de origen de identidad que permite incluir varios puntos de unión de Active Directory o agrupar una combinación de orígenes de identidad internos/externos, según se desee, que luego se enlaza a la directiva de autenticación bajo el Use columna.

El ejemplo que se muestra aquí permite que la búsqueda se realice primero en Active Directory y, si el usuario no se encuentra, busque en un servidor LDAP a continuación. Para varios orígenes de identidad, asegúrese siempre de que el **Treat as if the user was not found and proceed to the next store in the sequence** está activada. Esto es para que cada fuente/servidor de identidad se verifique durante la solicitud de autenticación.

Identity Source Sequences List > Identity_Sequence

Identity Source Sequence

Identity Source Sequence

* Name: Identity_Sequence

Description: [Empty text area]

: como mínimo, debe habilitar EAP-TLS, ya que ISE y nuestro solicitante se autentican mediante EAP-TLS en este ejemplo de configuración.

Dictionaryes Conditions **Results**

Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name Allowed_Protocols

Description

▼ Allowed Protocols

Authentication Bypass

Process Host Lookup ⓘ MAB

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow LEAP

Allow PEAP

Allow EAP-FAST

Allow EAP-TTLS

Allow TEAP

Preferred EAP Protocol: EAP-TLS ⓘ

EAP-TLS L-bit ⓘ

Allow weak ciphers for EAP ⓘ

Require Message-Authenticator for all RADIUS Requests ⓘ

Protocolos para permitir que ISE los utilice durante la solicitud de autenticación para el solicitante del terminal

Nota: el uso del protocolo EAP preferido establecido en el valor de EAP-TLS hace que ISE solicite el protocolo EAP-TLS como el primer protocolo ofrecido al suplicante IEEE 802.1x del terminal. Esta configuración es útil si pretende autenticarse a través de EAP-TLS con frecuencia en la mayoría de los terminales que se autentican con ISE.

Paso 9. Crear el perfil de autorización

El último elemento de directiva necesario para generar es el perfil de autorización, que se enlaza a la directiva de autorización y proporciona el nivel de acceso deseado. El perfil de autorización está enlazado a la directiva de autorización. Para configurarlo desde la GUI de ISE, vaya a **Policy > Policy Elements: Results > Authorization > Authorization Profiles** y haga clic en **Add**.

El perfil de autorización contiene una configuración que da como resultado atributos que se transfieren de ISE al NAD para una sesión RADIUS determinada, en la que estos atributos se utilizan para alcanzar el nivel deseado de acceso a la red.

Como se muestra aquí, simplemente pasa RADIUS Access-Accept como Access Type (Tipo de acceso), sin embargo, se pueden utilizar elementos adicionales en la autenticación inicial. Observe los detalles de atributos en la parte inferior, que contiene el resumen de los atributos que ISE envía al NAD cuando coincide con un perfil de autorización determinado.

. Estos están habilitados de forma predeterminada en ISE 3.x. Al instalar ISE, siempre hay definido un conjunto de políticas, que es el conjunto de políticas predeterminado. El conjunto de políticas predeterminado contiene reglas de autenticación, autorización y políticas de excepción predefinidas y predeterminadas.

Los conjuntos de políticas se configuran jerárquicamente, lo que permite al administrador de ISE agrupar políticas similares, en términos de intención, en diferentes conjuntos para su uso dentro de una solicitud de autenticación. Las políticas de personalización y agrupación son prácticamente ilimitadas. Como tal, se puede utilizar un conjunto de políticas para la autenticación de terminales inalámbricos para el acceso a la red, mientras que otro conjunto de políticas se puede utilizar para la autenticación de terminales por cable para el acceso a la red o para cualquier otra forma única y diferenciadora de gestionar políticas.

Cisco ISE puede evaluar los conjuntos de políticas y las políticas dentro de los usos del enfoque descendente para, en primer lugar, coincidir con un conjunto de políticas determinado cuando todas las condiciones de dicho conjunto se evalúan como verdaderas; sobre lo cual ISE evalúa, además, las políticas de autenticación y las políticas de autorización dentro de los usuarios que coinciden con el conjunto de políticas, de la siguiente manera:

1. Evaluación del conjunto de políticas y de las condiciones del conjunto de políticas
2. Políticas de autenticación dentro del conjunto de políticas coincidente
3. Directiva de autorización: excepciones locales
4. Política de autorización: excepciones globales
5. Políticas de autorización

Las excepciones de políticas existen globalmente para todos los conjuntos de políticas o localmente dentro de un conjunto de políticas específico. Estas excepciones de directiva se administran como parte de las directivas de autorización, ya que tratan de los permisos o resultados que se conceden para el acceso a la red en un escenario temporal determinado.

La siguiente sección trata sobre cómo combinar los elementos de configuración y políticas para enlazar con las Políticas de autenticación y autorización de ISE para autenticar un terminal a través de EAP-TLS.

Paso 10. Crear el conjunto de políticas

Un conjunto de directivas es un contenedor jerárquico que consta de una única regla definida por el usuario que indica el protocolo o la secuencia de servidor permitidos para el acceso a la red, así como las directivas de autenticación y autorización y las excepciones de directivas; todo ello también configurado con reglas basadas en condiciones definidas por el usuario.

Para crear un conjunto de políticas desde la GUI de ISE, navegue hasta **Policy > Policy Set** y, a continuación, haga clic en el icono más (+) de la esquina superior izquierda, como se muestra en esta imagen.

Policy Sets

Status	Policy Set Name	Description	Conditions
Search			

Adición de un nuevo conjunto de políticas

El conjunto de políticas puede enlazar/combinar este elemento de política previamente configurado y se utiliza para determinar qué conjunto de políticas debe coincidir en una solicitud de autenticación RADIUS (solicitud de acceso) dada:

- Enlazar: protocolos y servicios permitidos

Status	Policy Set Name	Description	Conditions
Search			
2)	EAP-TLS Example		3) AND RADIUS-Service-Type EQUALS Framed
			4) Network Access-Protocol EQUALS RADIUS
	Default	Default policy set	

Definición de Condiciones del Conjunto de Políticas y Lista de Protocolos Permitidos

Este ejemplo utiliza atributos y valores específicos que aparecerían en la sesión RADIUS para aplicar IEEE 802.1x (atributo enmarcado), aunque posiblemente sea redundante para volver a aplicar el protocolo RADIUS. Para obtener los mejores resultados, utilice sólo atributos de sesión RADIUS únicos que sean aplicables a la intención deseada, como Grupos de dispositivos de red o específicos para 802.1x por cable, 802.1x inalámbrico o tanto 802.1x por cable como 802.1x inalámbrico.

Puede encontrar más información sobre los conjuntos de políticas en ISE en las secciones Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Segmentación > [Conjuntos de políticas](#), [Políticas de autenticación](#) y [Políticas de autorización](#).

Paso 11. Crear una política de autenticación

Dentro del conjunto de directivas, la directiva de autenticación enlaza o combina estos elementos de directiva previamente configurados para utilizarse con condiciones para determinar cuándo debe coincidir una regla de autenticación.

- Enlazar: perfil de autenticación de certificado o secuencia de origen de identidad.

Status	Rule Name	Conditions
Search		

- Esto indica si la autenticación fue exitosa.
- En un escenario de trabajo, el valor es: Autenticación 5200 correcta.
- Nombre de usuario
 - Esto incluye la identidad final extraída del certificado de cliente presentado a ISE.
 - En un escenario de trabajo, este es el nombre de usuario del usuario conectado al terminal (es decir, employee1 de la imagen anterior).
- ID de terminal
 - Para redes por cable/inalámbricas, este valor es la dirección MAC de la tarjeta de interfaz de red (NIC) del terminal.
 - En un escenario de trabajo, se convierte en la dirección MAC del extremo a menos que la conexión se realice a través de VPN, en cuyo caso puede ser la dirección IP del extremo.
- Política de autenticación
 - Muestra la política de autenticación coincidente para la sesión dada en función de los atributos de sesión que coincidan con las condiciones de la política.
 - En un escenario de trabajo, esta es la política de autenticación esperada tal como está configurada.
 - Si ve otra política, significa que la política esperada cuando se compara con las condiciones en la política no fue evaluada como verdadera. En este caso, revise los atributos de sesión y asegúrese de que cada política contiene condiciones diferentes pero únicas para cada política.
- Política de autorización
 - Muestra la política de autorización coincidente para la sesión dada en función de los atributos de sesión que coincidan con las condiciones de la política.
 - En un escenario de trabajo, esta es la política de autorización esperada tal como está configurada.
 - Si ve otra directiva, significa que la directiva esperada, en comparación con las condiciones de la directiva, no se evaluó como verdadera. En este caso, revise los atributos de sesión y asegúrese de que cada política contiene condiciones diferentes, aunque únicas, para cada política.
- Resultado de autorización
 - Según la política de autorización coincidente, muestra el perfil de autorización que se utilizó en la sesión dada.
 - En un escenario de trabajo, este es el mismo valor que se configura en la política. Es recomendable realizar una revisión para fines de auditoría y asegurarse de que se ha configurado el perfil de autorización correcto.
- **Servidor de políticas**
 - Esto incluye el nombre de host del ISE Policy Service Node (PSN) que participó en el intento de autenticación.
 - En un escenario de trabajo, solo verá las autenticaciones que van al primer nodo PSN según lo configurado en el NAD (también conocido como dispositivo de borde), a menos que ese PSN no estuviera operativo o si se produjo un error, como debido a una latencia mayor de la esperada o si se produce un tiempo de espera de autenticación.
- método de autenticación
 - Muestra el método de autenticación que se utilizó en la sesión dada. Para este ejemplo, verá el valor como **dot1x**.
 - En un escenario de trabajo, basado en este ejemplo de configuración, verá el valor como **dot1x**. Si ve otro valor, podría significar que dot1x ha fallado o no se ha intentado.

- Protocolo de autenticación
 - Muestra el método de autenticación que se utilizó en la sesión dada. Para este ejemplo, verá el valor como EAP-TLS.
 - En un escenario de trabajo, basado en este ejemplo de configuración, siempre verá el valor como EAP-TLS. Si ve otro valor, el solicitante e ISE no negociaron correctamente EAP-TLS.
- Dispositivo de red
 - Muestra el nombre del dispositivo de red, tal y como se configura en ISE, para el NAD (también conocido como dispositivo de extremo) involucrado en el intento de autenticación entre el terminal e ISE.
 - En un escenario de trabajo, este nombre siempre se asigna en la interfaz de usuario de ISE: **Administration > System: Network Devices**. Según esa configuración, la dirección IP del NAD (también conocido como dispositivo de borde) se utiliza para determinar de qué dispositivo de red proviene la autenticación que se incluye en el atributo de sesión Dirección IPv4 del NAS.

No se trata en modo alguno de una lista completa de todos los atributos de sesión posibles que se deben revisar para solucionar problemas u otros fines de visibilidad, ya que hay otros atributos útiles que verificar. Se recomienda revisar todos los atributos de sesión para empezar a familiarizarse con toda la información. Puede ver la inclusión del lado derecho en la sección Pasos, que muestra las operaciones o el comportamiento que ha llevado a cabo ISE.

Problemas comunes y técnicas para solucionar problemas

Esta lista incluye algunos problemas comunes y consejos para la resolución de problemas, y de ninguna manera pretende ser una lista completa. En lugar de ello, utilícelo como guía y desarrolle sus propias técnicas para solucionar problemas cuando ISE esté involucrado.

Problema: se ha producido un error de autenticación (**error de autenticación 5400**) o cualquier otro intento de autenticación incorrecto.

- Si se encuentra un error de autenticación, haga clic en el icono **details** que brinda información sobre por qué falló la autenticación y los pasos realizados. Esto incluye el motivo de la falla y la posible causa raíz.
- Dado que ISE toma la decisión sobre el resultado de la autenticación, ISE dispone de la información necesaria para comprender el motivo por el que el intento de autenticación no tuvo éxito.

Problema: la autenticación no se completa correctamente y el motivo del error muestra "5440 Endpoint abandonó la sesión EAP e inició una nueva" o "5411 Supplicant dejó de responder a ISE".

- Este motivo de falla indica que la comunicación RADIUS no se completó antes de que se agotara el tiempo de espera. Dado que EAP está entre el terminal y NAD, debe verificar el tiempo de espera que se utiliza en NAD y asegurarse de que esté configurado durante al menos cinco segundos.
- Si cinco segundos no son suficientes para resolver este problema, se recomienda aumentarlo cinco segundos varias veces y volver a realizar la prueba para verificar si esta técnica resuelve el problema.
- Si el problema no se resuelve en los pasos anteriores, se recomienda asegurarse de que la autenticación la gestione el mismo nodo PSN de ISE correcto y de que el comportamiento general no sea indicativo de un comportamiento anormal, como una latencia superior a la normal entre los nodos PSN de ISE y NAD.

- Además, es una buena idea verificar si el terminal envía el certificado de cliente a través de la captura de paquetes si ISE no recibe el certificado de cliente, entonces el terminal (certificados de usuario) no puede confiar en el certificado de autenticación EAP de ISE. Si se determina que es true, importe la cadena de CA en los almacenes de certificados correctos (CA raíz = CA raíz de confianza) | Intermediario CA = Intermediario de confianza CA).

Problema: la autenticación es correcta, pero no coincide con la autenticación o la directiva de autorización correctas.

- Si encuentra una solicitud de autenticación exitosa, pero no coincide con las reglas de autenticación y/o autorización correctas, se recomienda revisar los atributos de sesión para asegurarse de que las condiciones utilizadas sean precisas y estén presentes en la sesión RADIUS.
- ISE evalúa estas políticas desde un enfoque descendente (con la excepción de las políticas de estado). En primer lugar, debe determinar si la política que coincidió estaba por encima o por debajo de la política que desea que coincida. La política de autenticación se evalúa primero e independientemente de las políticas de autorización. Si la política de autenticación coincide correctamente, entonces tiene 22037 Autenticación Pasada en los Detalles de autenticación bajo la sección derecha llamada Pasos.
- Si la política deseada está por encima de la política coincidente, esto significa que la suma de las condiciones en la política deseada no se evaluó como verdadera. Revisa todos los atributos y valores de la condición y de la sesión para asegurarse de que existe y de que no hay errores ortográficos.
- Si la política deseada está por debajo de la política coincidente, significa que se ha coincidido con otra política (anterior) en lugar de con la política deseada. Esto podría significar que los valores de condición no son lo suficientemente específicos, que las condiciones están duplicadas en otra política o que el orden de la política no es correcto. Aunque cada vez es más difícil resolver problemas, se recomienda empezar a revisar las políticas para determinar el motivo por el que no se ha coincidido la política deseada. Esto ayuda a identificar qué acciones tomar a continuación.

Problema: la identidad o el nombre de usuario utilizados durante la autenticación no eran el valor esperado.

- Cuando esto ocurre, si el terminal envía el certificado de cliente, lo más probable es que ISE no utilice el campo de certificado correcto en la plantilla de autenticación de certificados, que se evalúa durante la fase de autenticación.
- Revise el certificado de cliente para localizar el campo exacto en el que existe la identidad o el nombre de usuario deseados y asegúrese de que se ha seleccionado el mismo campo de: ISE UI: **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Problema: la autenticación no se realiza correctamente con el motivo del error **12514 EAP-TLS falló en el protocolo de enlace SSL/TLS debido a una CA desconocida en la cadena de certificados de cliente.**

- Esto puede ocurrir si el certificado de cliente tiene un certificado en la cadena de CA que no es de confianza en la interfaz de usuario de ISE: **Administration > System: Certificates > Trusted Certificates.**
- Esto suele ocurrir cuando el certificado de cliente (en el terminal) tiene una cadena de CA que es diferente de la cadena de CA de certificado que está firmada con ISE para la autenticación EAP.
- Para la resolución, asegúrese de que la cadena de CA del certificado de cliente sea de confianza en

ISE y de que la cadena de CA del certificado de servidor de autenticación EAP de ISE sea de confianza en el terminal.

- Para Windows OS y Chrome, diríjase a **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates**.

- Para Firefox: importe la cadena de CA (no el certificado de identidad final) de confianza para el servidor web.

Información Relacionada

- Cisco Identity Services Engine > [Guías de instalación y actualización](#)
- Cisco Identity Services Engine > [Guías de configuración](#)
- Cisco Identity Services Engine > [Información de compatibilidad](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Acceso seguro > [Definición de dispositivos de red en Cisco ISE](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Segmentación > [Conjuntos de políticas](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Segmentación > [Políticas de autenticación](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Segmentación > [Políticas de autorización](#)
- Cisco Identity Services Engine > Guías de configuración > [Integración de Active Directory con Cisco ISE 2.x](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Segmentación > Servicio de acceso a la red > [Acceso a la red para usuarios](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Configuración básica > [Administración de certificados en Cisco ISE](#)
- Guía del administrador de Cisco Identity Services Engine, versión 3.1 > Capítulo: Configuración básica > Cisco ISE CA Service > Configurar Cisco ISE para utilizar certificados para autenticar dispositivos personales > [Crear un perfil de autenticación de certificado para la autenticación basada en TLS](#)
- Cisco Identity Services Engine > Ejemplos de configuración y notas técnicas > [Configurar ISE 2.0 Certificate Provisioning Portal](#)
- Cisco Identity Services Engine > Ejemplos de configuración y notas técnicas > [Instalación de un certificado firmado por CA de terceros en ISE](#)
- LAN inalámbrica (WLAN) > Ejemplos de configuración y notas técnicas > [Comprensión y configuración de EAP-TLS mediante WLC e ISE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

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).