Configuración de cifrados en ISE 3.3 y versiones posteriores

Contenido

Introducción

Este documento describe cómo modificar los diferentes cifrados utilizados por ISE 3.3 y versiones posteriores en diferentes servicios para que el usuario tenga control sobre dichos mecanismos.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componente utilizado

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

- Cisco ISE versión 3.3.

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.

Conjuntos Cipher Soportados

Cisco ISE es compatible con las versiones 1.0, 1.1 y 1.2 de TLS.

Desde Cisco ISE Release 3.3, TLS 1.3 se introdujo solo para la GUI del administrador. Estos cifrados se soportan para el acceso HTTPS de administración sobre TL 1.3 :

- TLS_AES_128_GCM_SHA256

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE admite certificados de servidor RSA y ECDSA. Se admiten estas curvas elípticas:

- secp256r1
- secp384r1
- secp521r1

Esta tabla enumera las series Cipher soportadas:

Cipher Suite	Autenticación EAP/RADIUS DTLS	Descarga de CRL de HTTPS o comunicación de registro del sistema seguro/LDAP seguro/CoA de DTLS
ECDHE-ECDSA-AES256-GCM-SHA384	Sí, cuando TLS 1.1 está permitido.	Sí, cuando TLS 1.1 está permitido.
ECDHE-ECDSA-AES128-GCM-SHA256	Sí, cuando TLS 1.1 está permitido.	Sí, cuando TLS 1.1 está permitido.
ECDHE-ECDSA-AES256-SHA384	Sí, cuando TLS 1.1 está permitido.	Sí, cuando TLS 1.1 está permitido.
ECDHE-ECDSA-AES128-SHA256	Sí, cuando TLS 1.1 está permitido.	Sí, cuando TLS 1.1 está permitido.
ECDHE-ECDSA-AES256-SHA	Sí, cuando SHA-1 está permitido.	Sí, cuando SHA-1 está permitido.
ECDHE-ECDSA-AES128-SHA	Sí, cuando SHA-1 está permitido.	Sí, cuando SHA-1 está permitido.
ECDHE-RSA-AES256-GCM-SHA384	Sí, cuando se permite ECDHE-RSA.	Sí cuando se permite ECDHE-RSA.
ECDHE-RSA-AES128-GCM-SHA256	Sí, cuando se permite ECDHE-RSA.	Sí, cuando se permite ECDHE-RSA.

ECDHE-RSA-AES256-SHA384	Sí, cuando se permite ECDHE-RSA.	Sí, cuando se permite ECDHE-RSA.
ECDHE-RSA-AES128-SHA256	Sí, cuando se permite ECDHE-RSA.	Sí, cuando se permite ECDHE-RSA.
ECDHE-RSA-AES256-SHA	Sí, cuando se permite ECDHE-RSA/SHA-1.	Sí, cuando se permite ECDHE-RSA/SHA-1.
ECDHE-RSA-AES128-SHA	Sí, cuando se permite ECDHE-RSA/SHA-1.	Sí, cuando se permite ECDHE-RSA/SHA-1.
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	Sí, cuando SHA-1 está permitido.
DHE-RSA-AES128-SHA	No	Sí, cuando SHA-1 está permitido.
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	Sí, cuando SHA-1 está permitido.	Sí, cuando SHA-1 está permitido.
AES128-SHA	Sí, cuando SHA-1 está permitido.	Sí, cuando SHA-1 está permitido.
DES-CBC3-SHA	Sí, cuando se permite 3DES/SHA-1.	Sí, cuando se permite 3DES/SHA-1.
DHE-DSS-AES256-SHA	No	Sí, cuando 3DES/DSS y SHA-1 están activados.
DHE-DSS-AES128-SHA	No	Sí, cuando 3DES/DSS y SHA-1

		están activados.
EDH-DSS-DES-CBC3-SHA	No	Sí, cuando 3DES/DSS y SHA-1 están activados.
RC4-SHA	Cuando la opción Permitir cifrados débiles está habilitada en la página Protocolos permitidos y cuando SHA-1 está permitido.	No
RC4-MD5	Cuando la opción Permitir cifrados débiles está habilitada en la página Protocolos permitidos y cuando SHA-1 está permitido.	No
Solo aprovisionamiento anónimo de AP-FAST: ADH-AES-128-SHA	Yes	No
Validar KeyUsage	El certificado de cliente puede tener KeyUsage=Key Agreement y ExtendedKeyUsage=Client Authentication para estos cifrados: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validar ExtendedKeyUsage	El certificado de cliente debe tener KeyUsage=Key Encipherment y ExtendedKeyUsage=Client Authentication para estos	El certificado de servidor debe tener ExtendedKeyUsage=Autenticación de servidor.

	cifrados: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	

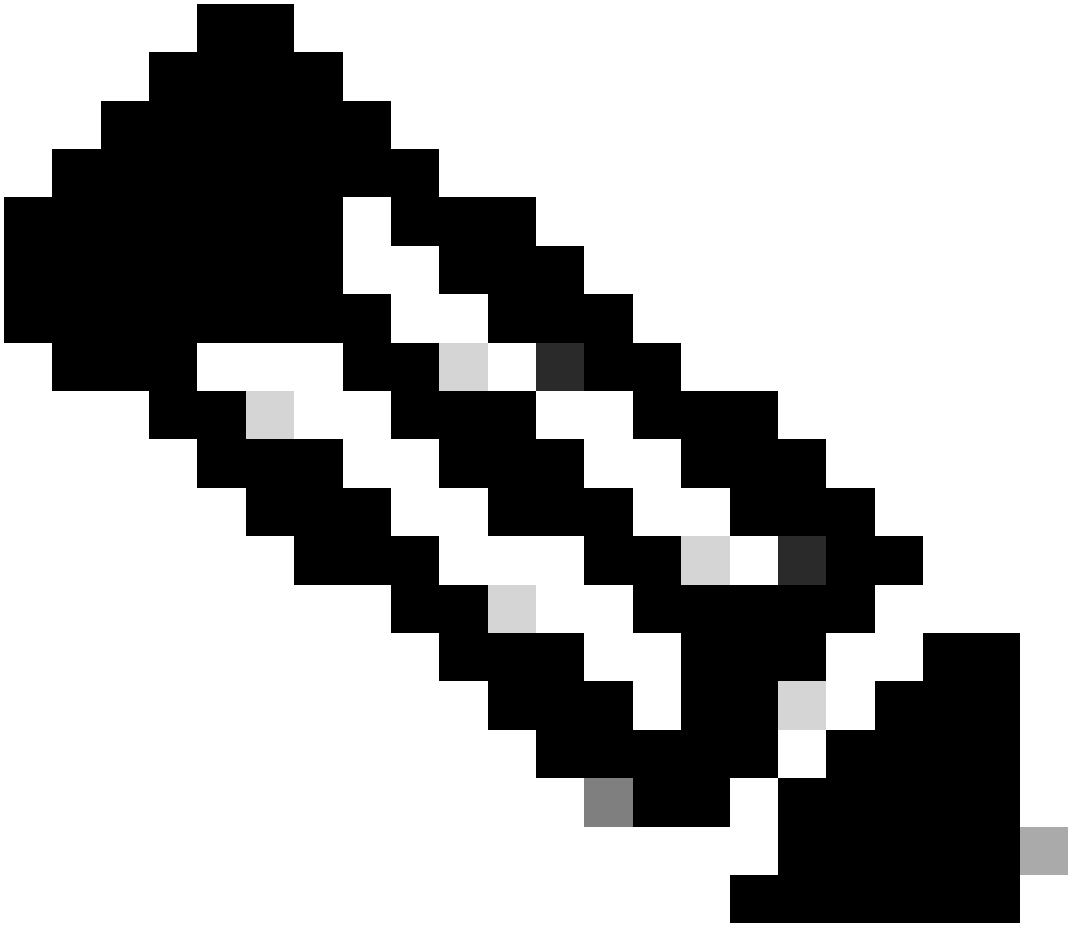
Configuraciones

Configurar los parámetros de seguridad

Realice este procedimiento para configurar los parámetros de seguridad:

1. En la GUI de Cisco ISE, haga clic en el icono del menú ( ) y seleccione Administration > System > Settings > Security Settings.

2. En la sección Configuración de versiones de TLS, elija una o varias versiones de TLS consecutivas. Marque la casilla de verificación situada junto a las versiones de TLS que desee habilitar.



Nota: TLS 1.2 está habilitado de forma predeterminada y no se puede deshabilitar. Si elige más de una versión de TLS, debe elegir versiones consecutivas. Por ejemplo, si elige TLS 1.0, TLS 1.1 se habilita automáticamente. Si cambia los cifrados aquí, puede reiniciar ISE.

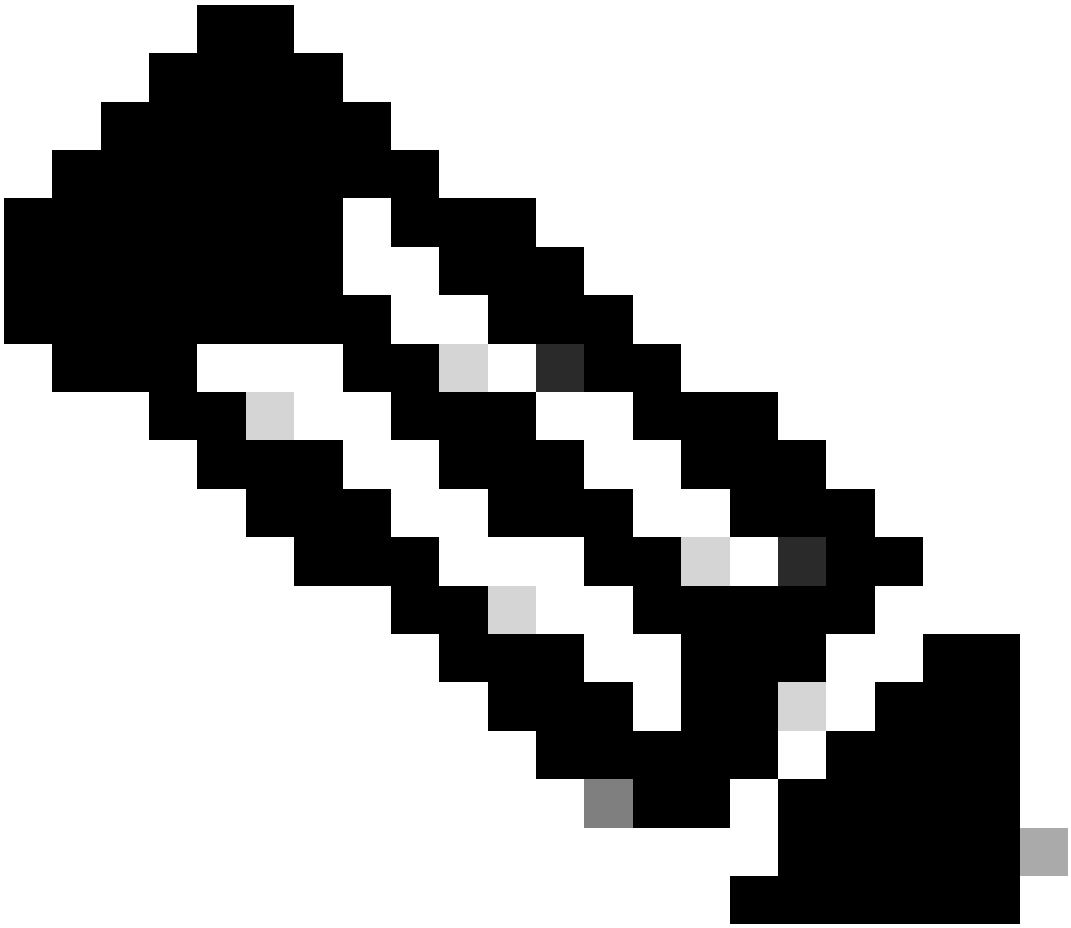
Permitir TLS 1.0, 1.1 y 1.2: habilita TLS 1.0, 1.1 y 1.2 para los siguientes servicios. Además, allow SHA-1 Ciphers: Permite a los cifradores SHA-1 comunicarse con peers para estos flujos de trabajo:

- Autenticación EAP.
- Descarga de CRL del servidor HTTPS.
- Comunicación de Syslog segura entre ISE y el servidor syslog externo.
- ISE como cliente LDAP seguro.
- ISE como cliente ODBC seguro.
- servicios ERS.
- servicios pxGrid.
- Todos los portales de ISE (por ejemplo, el portal de invitados, el portal de aprovisionamiento

de clientes o el portal Mis dispositivos).
- Comunicación de MDM.
- Comunicación con el agente PassiveID.
- Aprovisionamiento de la autoridad certificadora.
- Acceso GUI de administrador.

Estos puertos son utilizados por los componentes enumerados en la parte superior para la comunicación:

- Acceso de administrador: 443
- Portales de Cisco ISE: 9002, 8443, 8444, 8445, 8449 o cualquier puerto configurado para portales de ISE.
- ERS: 9060, 9061 y 9063
- pxGrid: 8910



Nota: La opción Allow SHA-1 Ciphers (Permitir cifrados SHA-1) está desactivada de

---

forma predeterminada. Recomendamos que utilice cifrados SHA-256 o SHA-384 para mejorar la seguridad.

Debe reiniciar todos los nodos de una implementación después de habilitar o deshabilitar la opción Permitir cifrados SHA-1. Si el reinicio no se realiza correctamente, no se aplican los cambios de configuración.

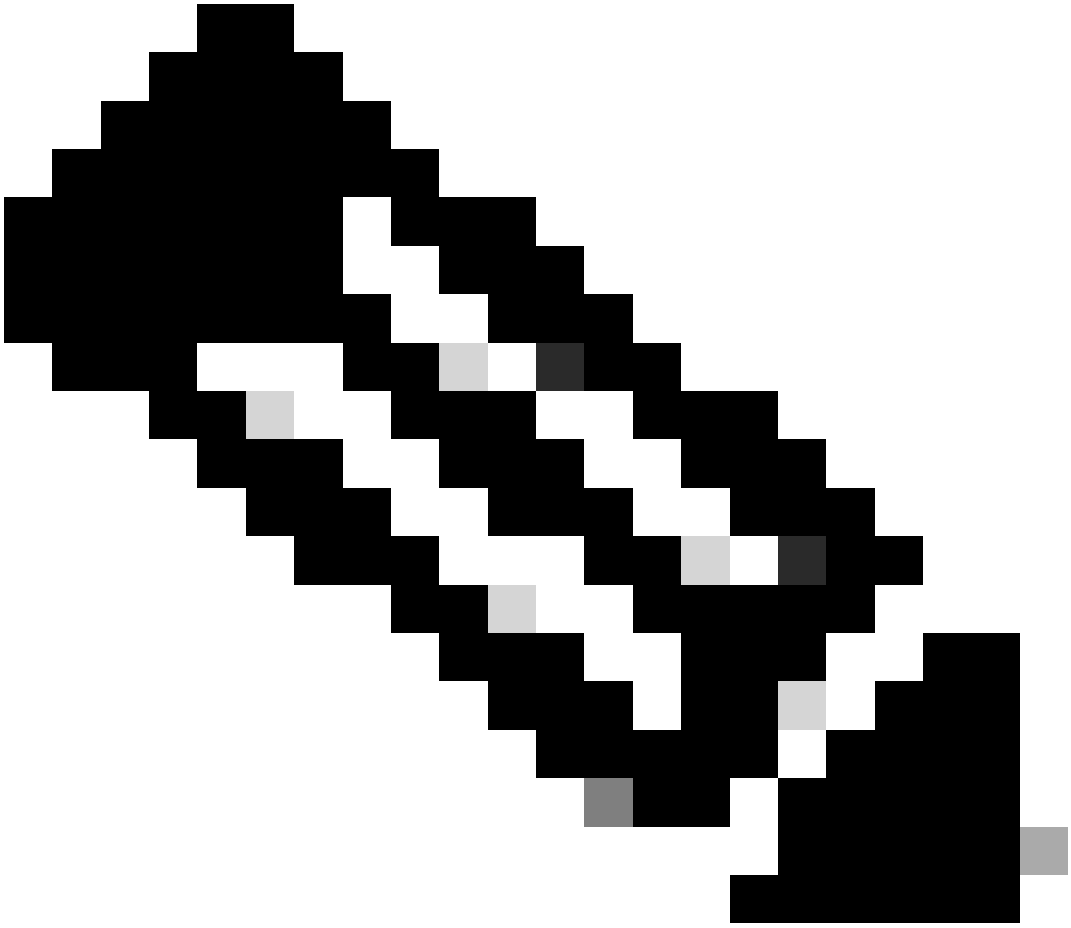
Cuando la opción Allow SHA-1 Ciphers está inhabilitada, si un cliente con solo cifrado SHA-1 intenta conectarse a Cisco ISE, el intercambio de señales falla y puede ver un mensaje de error en el navegador del cliente.

Elija una de las opciones y permita que los cifrados SHA-1 se comuniquen con los pares heredados:

- Permitir todos los cifrados SHA-1: permite que todos los cifrados SHA-1 se comuniquen con los pares heredados.
- Permitir sólo TLS_RSA_WITH_AES_128_CBC_SHA: permite sólo el cifrado TLS_RSA_WITH_AES_128_CBC_SHA para comunicarse con los pares heredados.

Permitir TLS 1.3: permite TLS 1.3 para el acceso HTTPS del administrador sobre el puerto 443 para:

- GUI de administración de Cisco ISE
- API habilitadas para el puerto 443 (API abierta, ERS, MnT).



Nota: las comunicaciones AAA y todos los tipos de comunicaciones entre nodos no admiten TLS 1.3. Habilite TLS 1.3 en Cisco ISE y los clientes y servidores relevantes para el acceso de administración a través de TLS 1.3.

Permitir cifrados ECDHE-RSA y 3DES: Permite a los cifradores ECDHE-RSA comunicarse con los pares para estos flujos de trabajo:

- Cisco ISE está configurado como servidor EAP
- Cisco ISE está configurado como servidor RADIUS DTLS
- Cisco ISE está configurado como cliente RADIUS DTLS
- Cisco ISE descarga CRL de HTTPS o un servidor LDAP seguro
- Cisco ISE está configurado como un cliente syslog seguro
- Cisco ISE está configurado como cliente LDAP seguro

Permitir cifrados DSS para ISE como cliente: cuando Cisco ISE actúa como cliente, permite a los cifradores DSS comunicarse con un servidor para estos flujos de trabajo:

- Cisco ISE está configurado como cliente RADIUS DTLS
- Cisco ISE descarga CRL de HTTPS o un servidor LDAP seguro
- Cisco ISE está configurado como un cliente syslog seguro
- Cisco ISE está configurado como cliente LDAP seguro

Permitir renegociación de TLS no seguro heredado para ISE como cliente: permite la comunicación con servidores TLS heredados que no admiten la renegociación de TLS segura para estos flujos de trabajo:

- Cisco ISE descarga CRL de HTTPS o un servidor LDAP seguro
- Cisco ISE está configurado como un cliente syslog seguro
- Cisco ISE está configurado como cliente LDAP seguro

Revelar nombres de usuario no válidos: de forma predeterminada, Cisco ISE muestra el mensaje no válido para los fallos de autenticación debido a nombres de usuario incorrectos. Para facilitar la depuración, esta opción obliga a Cisco ISE a mostrar los nombres de usuario en los informes, en lugar del mensaje no válido. Observe que los nombres de usuario siempre se muestran para las autenticaciones fallidas que no se deben a nombres de usuario incorrectos.

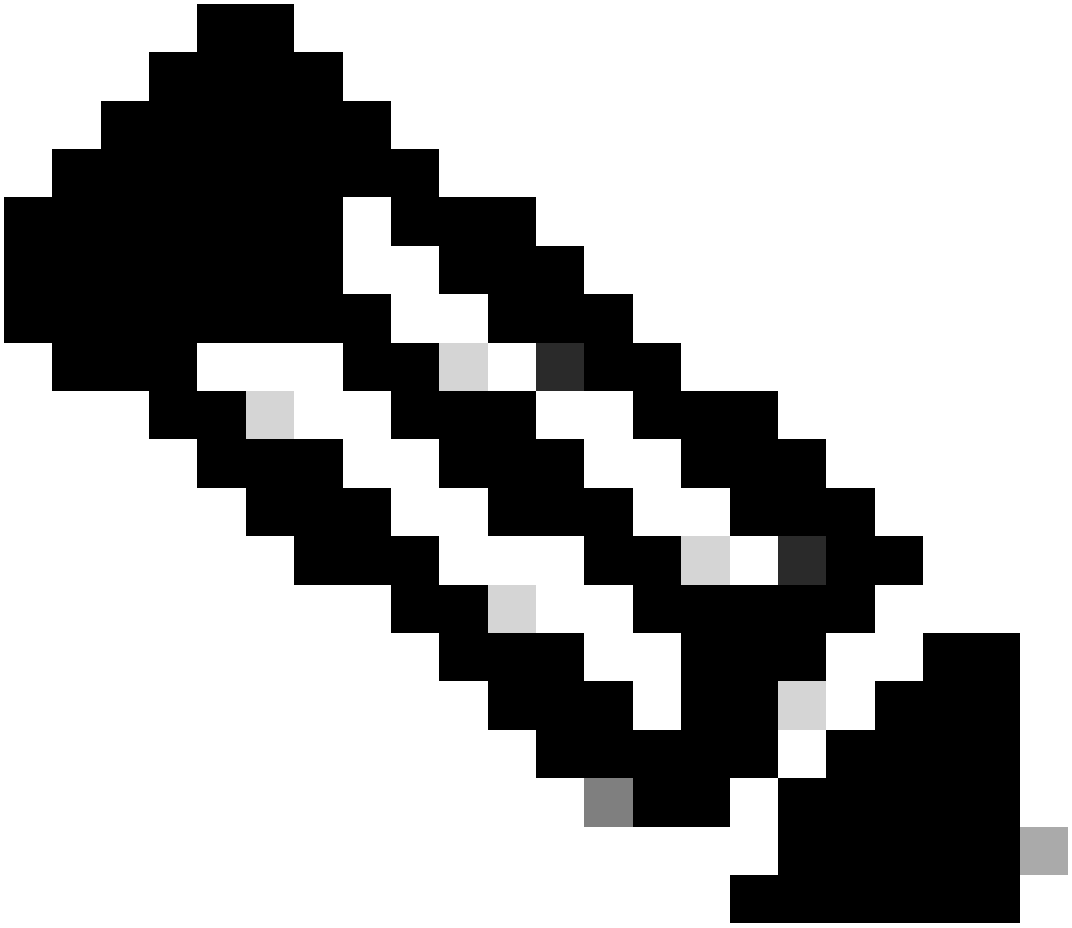
Esta característica es compatible con Active Directory, usuarios internos, LDAP y orígenes de identidad ODBC. No es compatible con otros orígenes de identidad, como token RADIUS, RSA o SAML.

Utilizar certificados basados en FQDN para la comunicación con proveedores externos (TC-NAC): Los certificados basados en FQDN deben cumplir estas reglas:

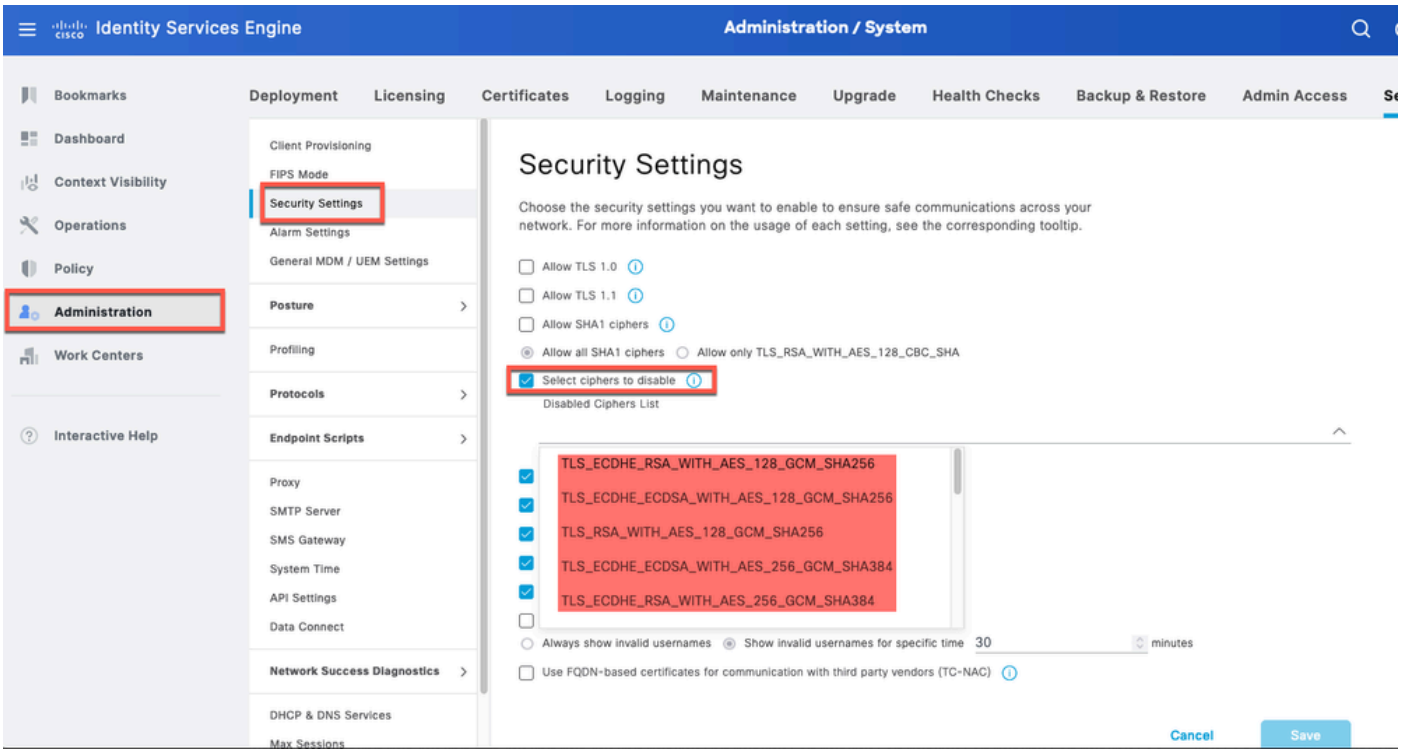
- Los campos SAN y CN del certificado deben contener valores FQDN. No se admiten nombres de host ni direcciones IP.
- Los certificados comodín deben contener el carácter comodín sólo en el fragmento del extremo izquierdo.
- El FQDN proporcionado en un certificado debe poder resolverse mediante DNS.

Deshabilitar Cifrados Específicos

Marque la opción Manually Configure Ciphers List si desea configurar manualmente los cifrados para comunicarse con estos componentes de Cisco ISE: admin UI, ERS, OpenAPI, secure ODBC, portals y pxGrid. Se muestra una lista de cifrados con los cifrados permitidos ya seleccionados. Por ejemplo, si la opción Allow SHA1 Ciphers está habilitada, los cifrados SHA1 están habilitados en esta lista. Si se selecciona la opción Allow Only TLS_RSA_WITH_AES_128_CBC_SHA, sólo se habilita este cifrado SHA1 en esta lista. Si la opción Allow SHA1 Ciphers está inhabilitada, no puede habilitar ningún cifrado SHA1 en este



Nota: Al editar la lista de cifrados que se van a desactivar, el servidor de aplicaciones se reinicia en todos los nodos de Cisco ISE. Cuando el modo FIPS está activado o desactivado, se reinician los servidores de aplicaciones de todos los nodos, lo que provoca un tiempo de inactividad significativo en el sistema. Si ha deshabilitado los cifrados mediante la opción Manually Configure Ciphers List, compruebe la lista de cifrados deshabilitados después de reiniciar los servidores de aplicaciones. La lista de cifrados deshabilitados no se cambia debido a la transición del modo FIPS.



Opción para deshabilitar Ciphers ISE 3.3

- Desde ISE CLI, puede ejecutar el comando application configure isey utilizar la opción 37, resaltada en esta captura de pantalla, **Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS**. El bug relacionado es el ID de bug de Cisco CSCwb7915.

```
isedemo-33/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
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
```

Opción para Inhabilitar/Habilitar RSA_PSS para EAP-TLS

Información Relacionada

-

Soporte técnico y descargas de Cisco

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).