Configurar cifras no ISE 3.3 e posterior

Contents

Introdução

Este documento descreve como modificar as diferentes cifras usadas pelo ISE 3.3 e posterior em diferentes serviços para que o usuário tenha controle sobre tais mecanismos.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componente usado

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 3.3.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conjuntos de cifras suportados

O Cisco ISE suporta TLS versões 1.0, 1.1 e 1.2.

A partir do Cisco ISE versão 3.3, o TLS 1.3 foi introduzido somente para GUI Admin. Essas cifras são suportadas para acesso HTTPS de admin sobre TL 1.3:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

O Cisco ISE suporta certificados de servidor RSA e ECDSA. Estas curvas elípticas são suportadas:

- secp256r1
- secp384r1
- secp521r1

Esta tabela lista os Conjuntos de Cifras suportados:

Conjunto de Cifras	Autenticação EAP/DTLS RADIUS	Download de CRL de HTTPS ou LDAP seguro/comunicação Syslog segura/DTLS CoA
ECDHE-ECDSA-AES256-GCM-SHA384	Sim, quando TLS 1.1 é permitido.	Sim, quando TLS 1.1 é permitido.
ECDHE-ECDSA-AES128-GCM-SHA256	Sim, quando TLS 1.1 é permitido.	Sim, quando TLS 1.1 é permitido.
ECDHE-ECDSA-AES256-SHA384	Sim, quando TLS 1.1 é permitido.	Sim, quando TLS 1.1 é permitido.
ECDHE-ECDSA-AES128-SHA256	Sim, quando TLS 1.1 é permitido.	Sim, quando TLS 1.1 é permitido.
ECDHE-ECDSA-AES256-SHA	Sim, quando SHA-1 é permitido.	Sim, quando SHA-1 é permitido.
ECDHE-ECDSA-AES128-SHA	Sim, quando SHA-1 é permitido.	Sim, quando SHA-1 é permitido.
ECDHE-RSA-AES256-GCM-SHA384	Sim, quando ECDHE-RSA é permitido.	Sim, quando ECDHE-RSA é permitido.
ECDHE-RSA-AES128-GCM-SHA256	Sim, quando ECDHE-RSA é permitido.	Sim, quando ECDHE-RSA é permitido.
ECDHE-RSA-AES256-SHA384	Sim, quando ECDHE-RSA é permitido.	Sim, quando ECDHE-RSA é permitido.

ECDHE-RSA-AES128-SHA256	Sim, quando ECDHE-RSA é permitido.	Sim, quando ECDHE-RSA é permitido.
ECDHE-RSA-AES256-SHA	Sim, quando ECDHE-RSA/SHA-1 é permitido.	Sim, quando ECDHE-RSA/SHA-1 é permitido.
ECDHE-RSA-AES128-SHA	Sim, quando ECDHE-RSA/SHA-1 é permitido.	Sim, quando ECDHE-RSA/SHA-1 é permitido.
DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	Sim, quando SHA-1 é permitido.
DHE-RSA-AES128-SHA	No	Sim, quando SHA-1 é permitido.
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	Sim, quando SHA-1 é permitido.	Sim, quando SHA-1 é permitido.
AES128-SHA	Sim, quando SHA-1 é permitido.	Sim, quando SHA-1 é permitido.
DES-CBC3-SHA	Sim, quando 3DES/SHA-1 for permitido.	Sim, quando 3DES/SHA-1 for permitido.
DHE-DSS-AES256-SHA	No	Sim, quando 3DES/DSS e SHA-1 estão ativados.
DHE-DSS-AES128-SHA	No	Sim, quando 3DES/DSS e SHA-1 estão ativados.

EDH-DSS-DES-CBC3-SHA	No	Sim, quando 3DES/DSS e SHA-1 estão ativados.
RC4-SHA	Quando a opção Permitir cifras fracas estiver habilitada na página Protocolos permitidos e quando SHA-1 for permitido.	No
RC4-MD5	Quando a opção Permitir cifras fracas estiver habilitada na página Protocolos permitidos e quando SHA-1 for permitido.	No
Somente provisionamento anônimo AP-FAST: ADH-AES-128-SHA	Yes	No
Validar KeyUsage	O certificado do cliente pode ter KeyUsage=Key Agreement e ExtendedKeyUsage=Client Authentication para estas cifras: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validar ExtendedKeyUsage	O certificado do cliente deve ter KeyUsage=KeyUsage e ExtendedKeyUsage=Client Authentication para estas codificações: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	O certificado do servidor deve ter ExtendedKeyUsage=Server Authentication.

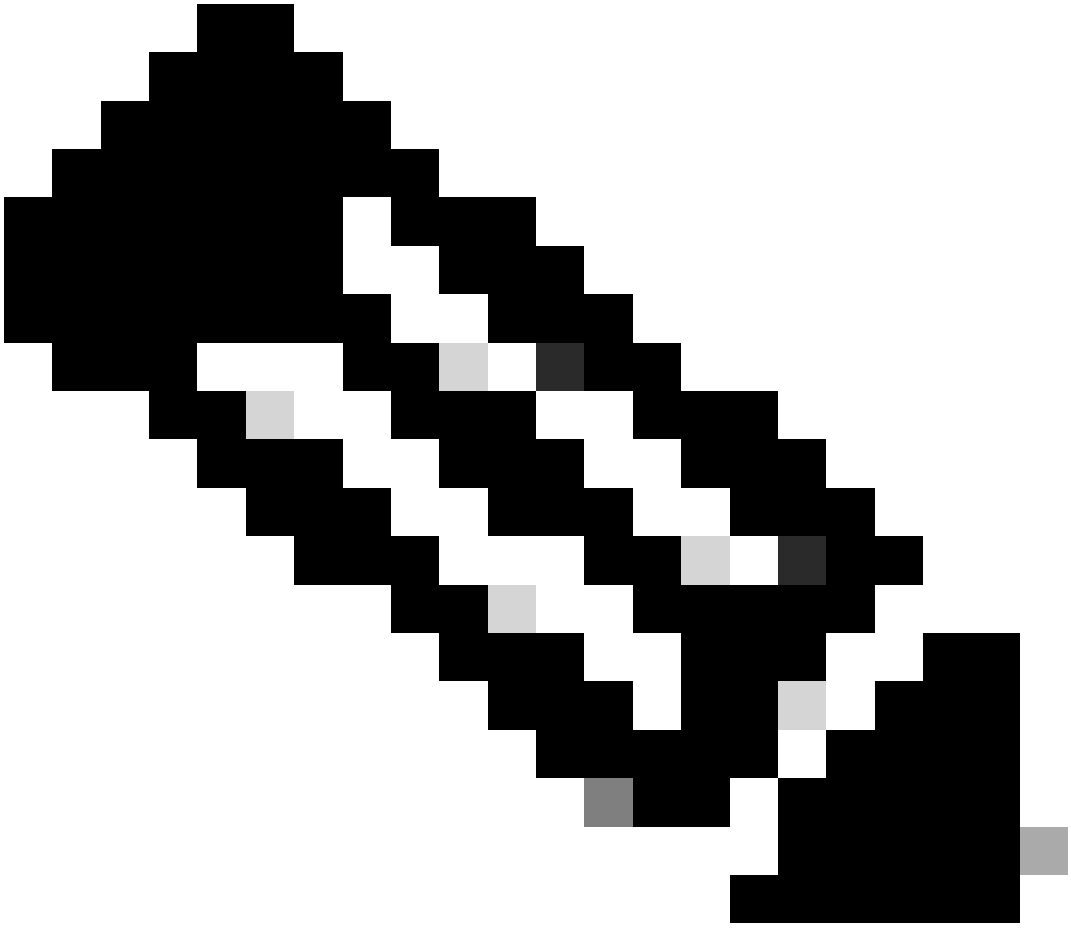
Configurações

Definir configurações de segurança

Execute este procedimento para definir as configurações de segurança:

1. Na GUI do Cisco ISE, clique no ícone de menu () e escolha Administration > System > Settings > Security Settings.

2. Na seção Configurações de versões de TLS, escolha uma ou várias versões de TLS consecutivas. Marque a caixa de seleção ao lado das versões de TLS que deseja ativar.



Observação: TLS 1.2 está habilitado por padrão e não pode ser desabilitado. Se você escolher mais de uma versão de TLS, deverá escolher versões consecutivas. Por exemplo, se você escolher TLS 1.0, TLS 1.1 será habilitado automaticamente. Alterar as cifras aqui pode causar a reinicialização do ISE.

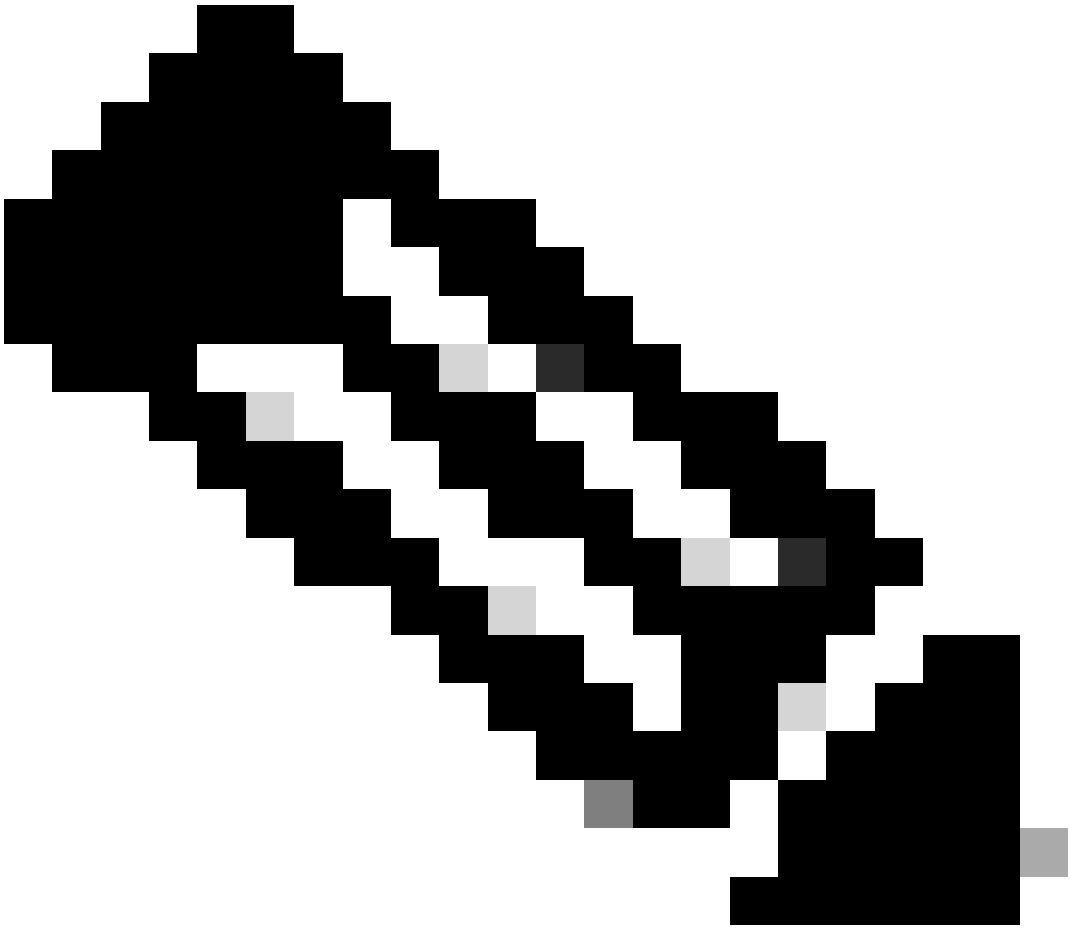
Permitir TLS 1.0, 1.1 e 1.2: Ativa TLS 1.0, 1.1 e 1.2 para os próximos serviços. Além disso, permitir cifras SHA-1: permite que as cifras SHA-1 se comuniquem com os pares para estes fluxos de trabalho:

- Autenticação EAP.
- Download de CRL do servidor HTTPS.
- Comunicação segura de Syslog entre o ISE e o servidor syslog externo.
- ISE como um cliente LDAP seguro.
- ISE como um cliente ODBC seguro.
- Serviços ERS.
- serviços pxGrid.
- Todos os portais do ISE (por exemplo, Portal de convidados, Portal de provisionamento de

clientes, Portal MyDevices).
- Comunicação MDM.
- Comunicação do PassiveID Agent.
- Provisionamento da Autoridade de Certificação.
- Admin GUI Access (Acesso à GUI do Administrador).

Essas portas são usadas pelos componentes listados na parte superior para comunicação:

- Acesso administrativo: 443
- Portais do Cisco ISE: 9002, 8443, 8444, 8445, 8449 ou qualquer porta configurada para portais do ISE.
- ERS: 9060, 9061, 9063
- pxGrid: 8910



Observação: a opção Permitir cifras SHA-1 está desabilitada por padrão. Recomendamos que você use cifras SHA-256 ou SHA-384 para maior segurança.

Você deve reiniciar todos os nós em uma implantação após habilitar ou desabilitar a opção Permitir Cifras SHA-1. Se a reinicialização não for bem-sucedida, as alterações de configuração não serão aplicadas.

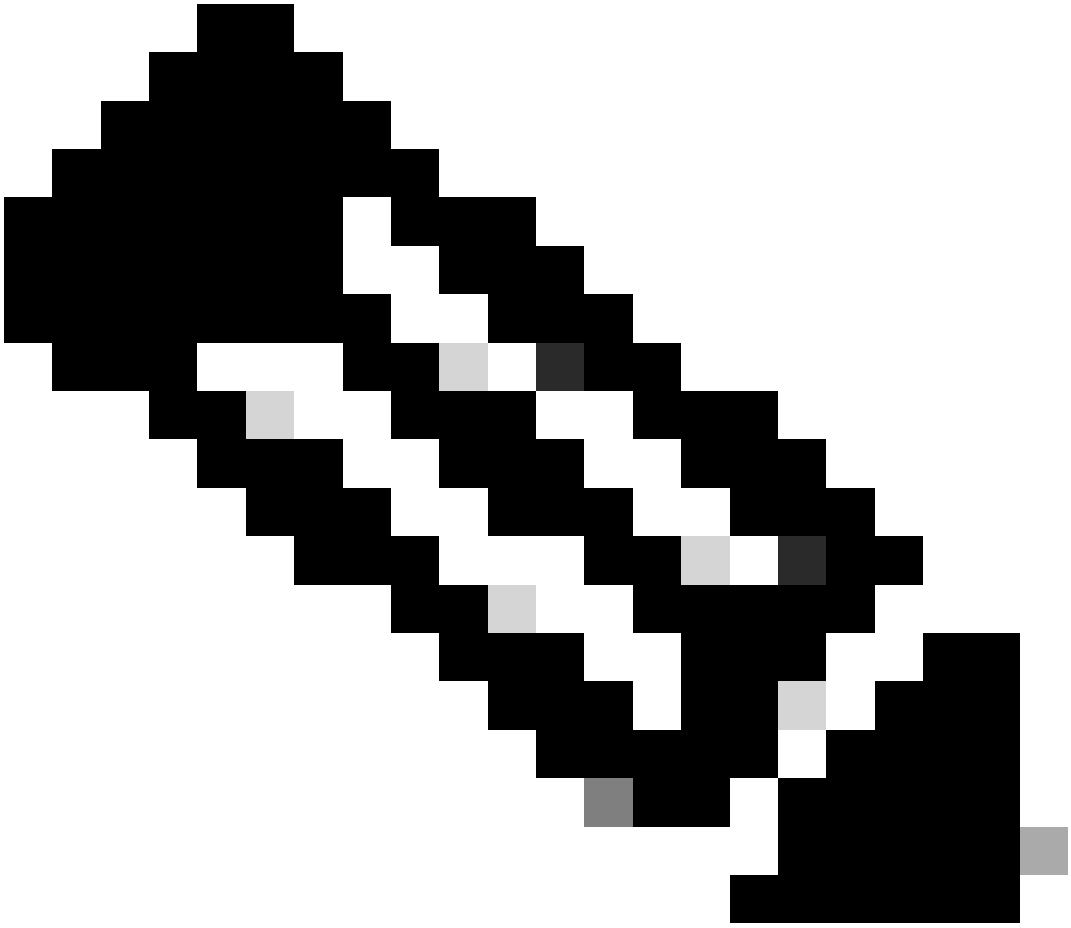
Quando a opção Permitir cifras SHA-1 estiver desativada, se um cliente com apenas cifras SHA-1 tentar se conectar ao Cisco ISE, o handshake falhará e você poderá ver uma mensagem de erro no navegador do cliente.

Escolha uma das opções enquanto permite que as cifras SHA-1 se comuniquem com os pares legados:

- Permitir todas as cifras SHA-1: Permite que todas as cifras SHA-1 se comuniquem com os pares legados.
- Permitir apenas TLS_RSA_WITH_AES_128_CBC_SHA: Permite apenas que a cifra TLS_RSA_WITH_AES_128_CBC_SHA se comunique com os peers herdados.

Permitir TLS 1.3: Permite TLS 1.3 para acesso HTTPS de administrador pela porta 443 para:

- GUI de administração do Cisco ISE
- APIs habilitadas para a porta 443 (API aberta, ERS, MnT).



Observação: as comunicações AAA e todos os tipos de comunicações entre nós não suportam TLS 1.3. Ative o TLS 1.3 no Cisco ISE e nos clientes e servidores relevantes para acesso de administrador sobre o TLS 1.3.

Permitir Cifras ECDHE-RSA e 3DES: Permite que as cifras ECDHE-RSA se comuniquem com os pares para estes fluxos de trabalho:

- O Cisco ISE está configurado como um servidor EAP
- O Cisco ISE está configurado como um servidor RADIUS DTLS
- O Cisco ISE está configurado como um cliente RADIUS DTLS
- O Cisco ISE baixa CRL de HTTPS ou de um servidor LDAP seguro
- O Cisco ISE está configurado como um cliente syslog seguro
- O Cisco ISE está configurado como um cliente LDAP seguro

Permitir cifras DSS para o ISE como cliente: quando o Cisco ISE atua como cliente, permite que as cifras DSS se comuniquem com um servidor para estes fluxos de trabalho:

- O Cisco ISE está configurado como um cliente RADIUS DTLS
- O Cisco ISE baixa CRL de HTTPS ou de um servidor LDAP seguro
- O Cisco ISE está configurado como um cliente syslog seguro
- O Cisco ISE está configurado como um cliente LDAP seguro

Permitir renegociação TLS sem segurança herdada para ISE como um cliente: Permite a comunicação com servidores TLS herdados que não oferecem suporte à renegociação TLS segura para estes fluxos de trabalho:

- O Cisco ISE baixa CRL de HTTPS ou de um servidor LDAP seguro
- O Cisco ISE está configurado como um cliente syslog seguro
- O Cisco ISE está configurado como um cliente LDAP seguro

Divulgar nomes de usuário inválidos: por padrão, o Cisco ISE exibe a mensagem inválida para falhas de autenticação devido a nomes de usuário incorretos. Para auxiliar na depuração, essa opção força o Cisco ISE a exibir nomes de usuário em relatórios, em vez de mensagens inválidas. Observe que os nomes de usuário são sempre exibidos para autenticações com falha que não são devido a nomes de usuário incorretos.

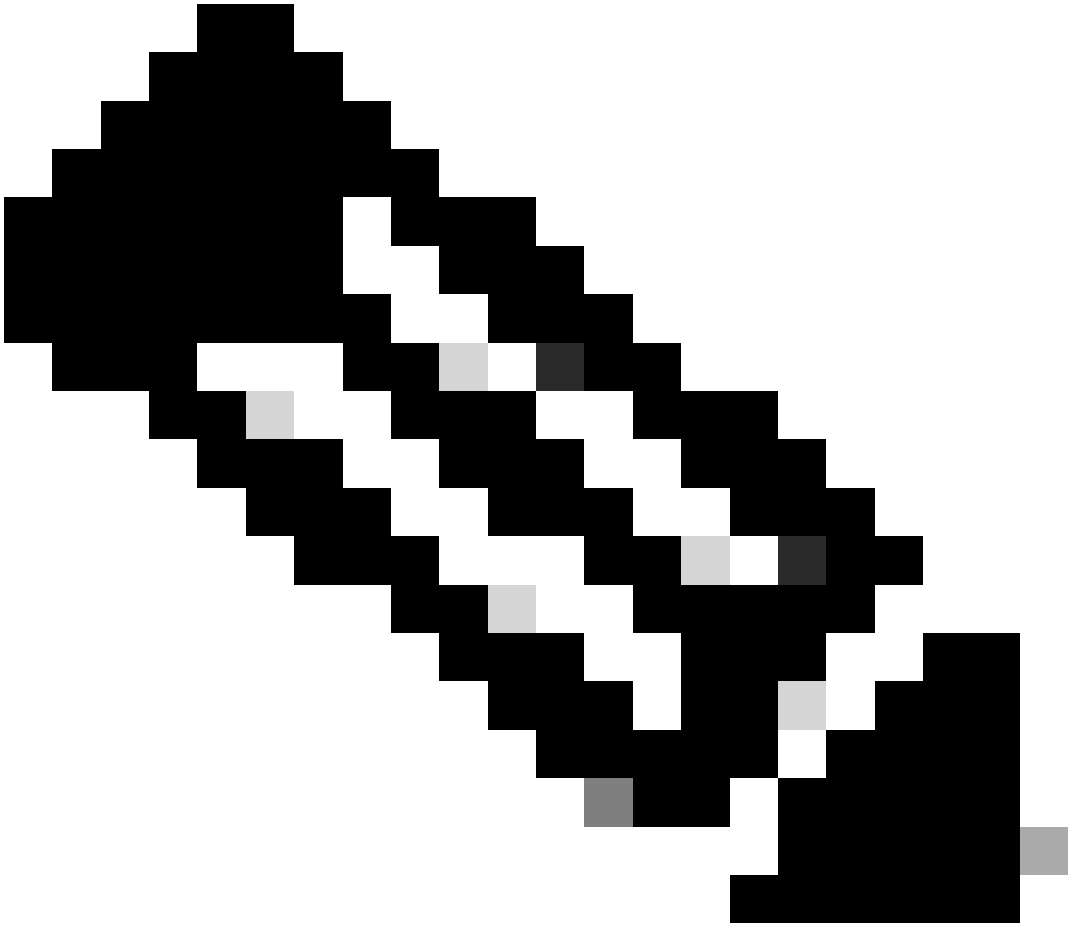
Este recurso é suportado para origens de identidade Ative Diretory, Usuários Internos, LDAP e ODBC. Não há suporte para outras fontes de identidade, como token RADIUS, RSA ou SAML.

Usar certificados baseados em FQDN para comunicação com fornecedores terceirizados (TC-NAC): Os certificados baseados em FQDN devem estar em conformidade com estas regras:

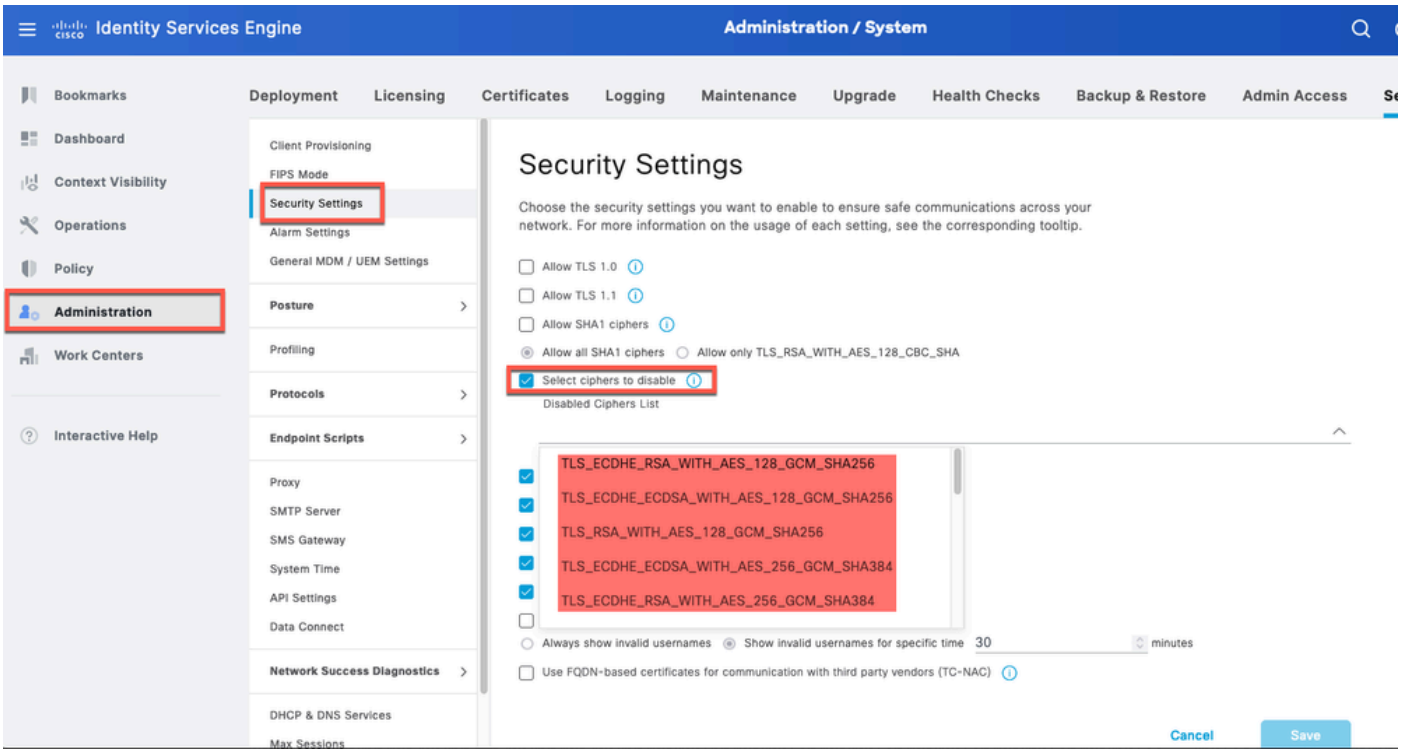
- Os campos SAN e CN no certificado devem conter valores FQDN. Não há suporte para nomes de host e endereços IP.
- Os certificados curinga devem conter o caractere curinga apenas no fragmento da extremidade esquerda.
- O FQDN fornecido em um certificado deve ser resolvível pelo DNS.

Desativar cifras específicas

Marque a opção Manually Configure Ciphers List se quiser configurar manualmente as cifras para se comunicar com esses componentes do Cisco ISE: admin UI, ERS, OpenAPI, ODBC seguro, portais e pxGrid. Uma lista de cifras é exibida com as cifras permitidas já selecionadas. Por exemplo, se a opção Permitir cifras SHA1 estiver habilitada, as cifras SHA1 serão habilitadas nessa lista. Se a opção Permitir somente TLS_RSA_WITH_AES_128_CBC_SHA estiver selecionada, somente esta cifra SHA1 será habilitada nesta lista. Se a opção Permitir cifras SHA1 estiver desativada, você não poderá ativar nenhuma cifra SHA1 neste

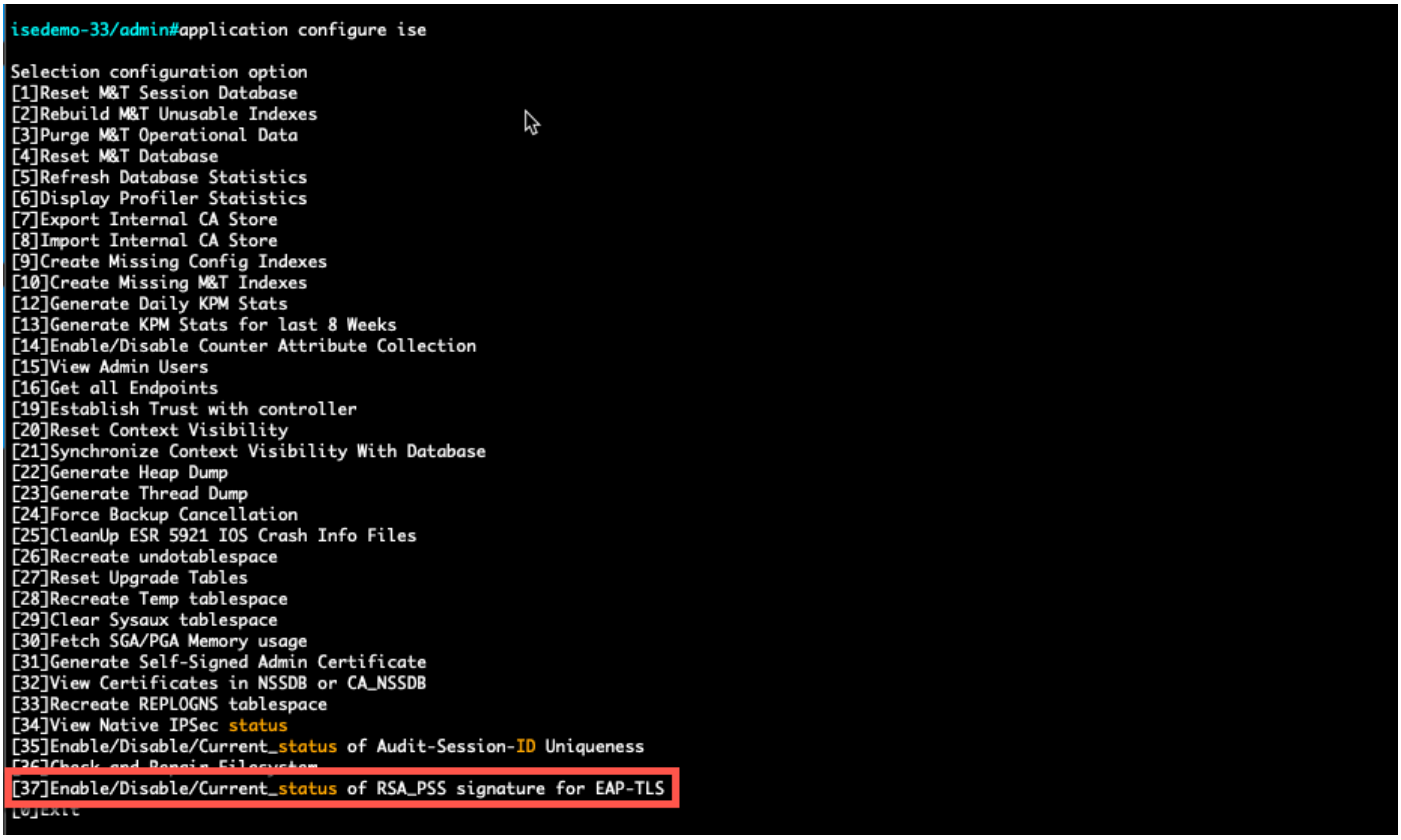


Observação: quando você edita a lista de cifras a serem desativadas, o servidor de aplicativos é reiniciado em todos os nós do Cisco ISE. Quando o modo FIPS é ativado ou desativado, os servidores de aplicativos em todos os nós são reiniciados, resultando em um tempo de inatividade significativo do sistema. Se você desativou qualquer cifra usando a opção Configurar manualmente a lista de cifras, verifique a lista de cifras desativadas depois que os servidores de aplicativos forem reiniciados. A lista de cifras desabilitada não foi alterada devido à transição do modo FIPS.



Opção de desativar as cifras do ISE 3.3

- Na CLI do ISE, você pode executar o comando application configure isee usar a Opção 37, destacada nesta captura de tela, **Enable/Disable/Current_status da assinatura RSA_PSS para EAP-TLS**. O bug relacionado é o ID de bug da Cisco CSCwb7915.



Opção para desativar/ativar RSA_PSS para EAP-TLS

Informações Relacionadas

-

Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.