Configuration du chiffrement dans ISE 3.3 et versions ultérieures

Table des matières

Introduction

Ce document décrit comment modifier les différents chiffrements utilisés par ISE 3.3 et versions ultérieures dans différents services afin que les utilisateurs aient le contrôle sur de tels mécanismes.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composant utilisé

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Suites de chiffrement prises en charge

Cisco ISE prend en charge les versions TLS 1.0, 1.1 et 1.2.

À partir de Cisco ISE version 3.3, TLS 1.3 a été introduit pour l'interface utilisateur graphique Admin uniquement. Ces chiffrements sont pris en charge pour l'accès HTTPS admin sur TL 1.3 :

- TLS_AES_128_GCM_SHA256

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE prend en charge les certificats de serveur RSA et ECDSA. Les courbes elliptiques suivantes sont prises en charge :

- secp256r1
- secp384r1
- secp521r1

Ce tableau répertorie les suites de chiffrement prises en charge :

Suite de chiffrement	Authentification EAP/RADIUS DTLS	Téléchargement CRL depuis HTTPS ou Secure LDAP/Secure Syslog communication/DTLS CoA
ECDHE-ECDSA-AES256-GCM-SHA384	Oui, lorsque TLS 1.1 est autorisé.	Oui, lorsque TLS 1.1 est autorisé.
ECDHE-ECDSA-AES128-GCM-SHA256	Oui, lorsque TLS 1.1 est autorisé.	Oui, lorsque TLS 1.1 est autorisé.
ECDHE-ECDSA-AES256-SHA384	Oui, lorsque TLS 1.1 est autorisé.	Oui, lorsque TLS 1.1 est autorisé.
ECDHE-ECDSA-AES128-SHA256	Oui, lorsque TLS 1.1 est autorisé.	Oui, lorsque TLS 1.1 est autorisé.
ECDHE-ECDSA-AES256-SHA	Oui, lorsque SHA-1 est autorisé.	Oui, lorsque SHA-1 est autorisé.
ECDHE-ECDSA-AES128-SHA	Oui, lorsque SHA-1 est autorisé.	Oui, lorsque SHA-1 est autorisé.
ECDHE-RSA-AES256-GCM-SHA384	Oui, lorsque ECDHE-RSA est autorisé.	Oui lorsque ECDHE-RSA est autorisé.
ECDHE-RSA-AES128-GCM-	Oui, lorsque ECDHE-RSA est	Oui, lorsque ECDHE-RSA est

SHA256	autorisé.	autorisé.
ECDHE-RSA-AES256-SHA384	Oui, lorsque ECDHE-RSA est autorisé.	Oui, lorsque ECDHE-RSA est autorisé.
ECDHE-RSA-AES128-SHA256	Oui, lorsque ECDHE-RSA est autorisé.	Oui, lorsque ECDHE-RSA est autorisé.
ECDHE-RSA-AES256-SHA	Oui, lorsque ECDHE-RSA/SHA-1 est autorisé.	Oui, lorsque ECDHE-RSA/SHA-1 est autorisé.
ECDHE-RSA-AES128-SHA	Oui, lorsque ECDHE-RSA/SHA-1 est autorisé.	Oui, lorsque ECDHE-RSA/SHA-1 est autorisé.
DHE-RSA-AES256-SHA256	Non	Oui
DHE-RSA-AES128-SHA256	Non	Oui
DHE-RSA-AES256-SHA	Non	Oui, lorsque SHA-1 est autorisé.
DHE-RSA-AES128-SHA	Non	Oui, lorsque SHA-1 est autorisé.
AES256-SHA256	Oui	Oui
AES128-SHA256	Oui	Oui
AES256-SHA	Oui, lorsque SHA-1 est autorisé.	Oui, lorsque SHA-1 est autorisé.
AES128-SHA	Oui, lorsque SHA-1 est autorisé.	Oui, lorsque SHA-1 est autorisé.
DES-CBC3-SHA	Oui, lorsque 3DES/SHA-1 est autorisé.	Oui, lorsque 3DES/SHA-1 est autorisé.

DHE-DSS-AES256-SHA	Non	Oui, lorsque 3DES/DSS et SHA-1 sont activés.
DHE-DSS-AES128-SHA	Non	Oui, lorsque 3DES/DSS et SHA-1 sont activés.
EDH-DSS-DES-CBC3-SHA	Non	Oui, lorsque 3DES/DSS et SHA-1 sont activés.
RC4-SHA	Lorsque l'option Allow faible ciphers est activée dans la page Allowed Protocols et lorsque SHA-1 est autorisé.	Non
RC4-MD5	Lorsque l'option Allow faible ciphers est activée dans la page Allowed Protocols et lorsque SHA-1 est autorisé.	Non
Approvisionnement anonyme AP-FAST uniquement : ADH-AES-128-SHA	Oui	Non
Valider l'utilisation des clés	Le certificat client peut avoir KeyUsage=Key Agreement et ExtendedKeyUsage=Client Authentication pour ces chiffrements : • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Valider ExtendedKeyUsage	Le certificat client doit avoir KeyUsage=Key Encipherment et ExtendedKeyUsage=Client Authentication pour ces	Le certificat de serveur doit avoir ExtendedKeyUsage=Server Authentication.

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

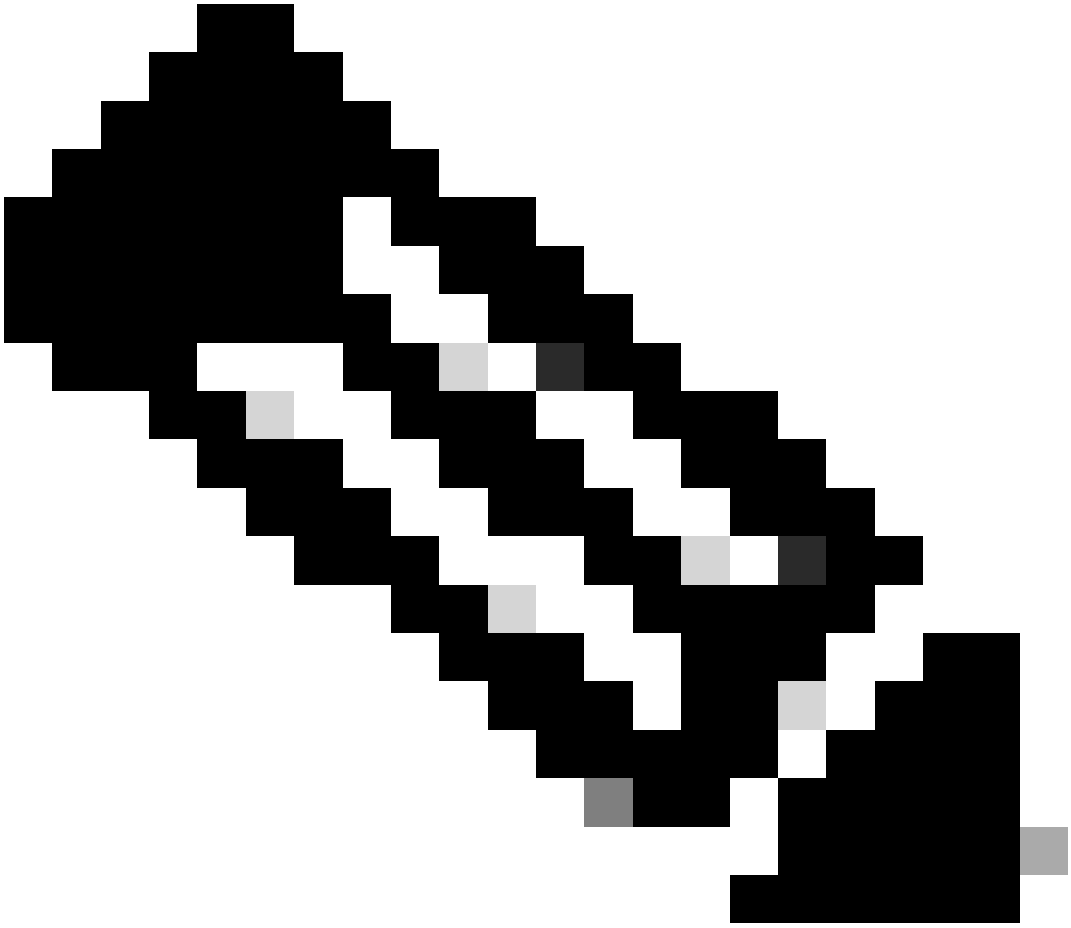
Configurations

Configuration des paramètres de sécurité

Procédez comme suit pour configurer les paramètres de sécurité :

1. Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône de menu ( ) et choisissez Administration > System > Settings > Security Settings.

2. Dans la section Paramètres des versions TLS, choisissez une ou une plage de versions TLS consécutives. Cochez la case en regard des versions TLS que vous souhaitez activer.



Remarque : TLS 1.2 est activé par défaut et ne peut pas être désactivé. Si vous choisissez plusieurs versions TLS, vous devez choisir des versions consécutives. Par exemple, si vous choisissez TLS 1.0, TLS 1.1 est automatiquement activé. La modification des chiffres ici peut entraîner le redémarrage d'ISE.

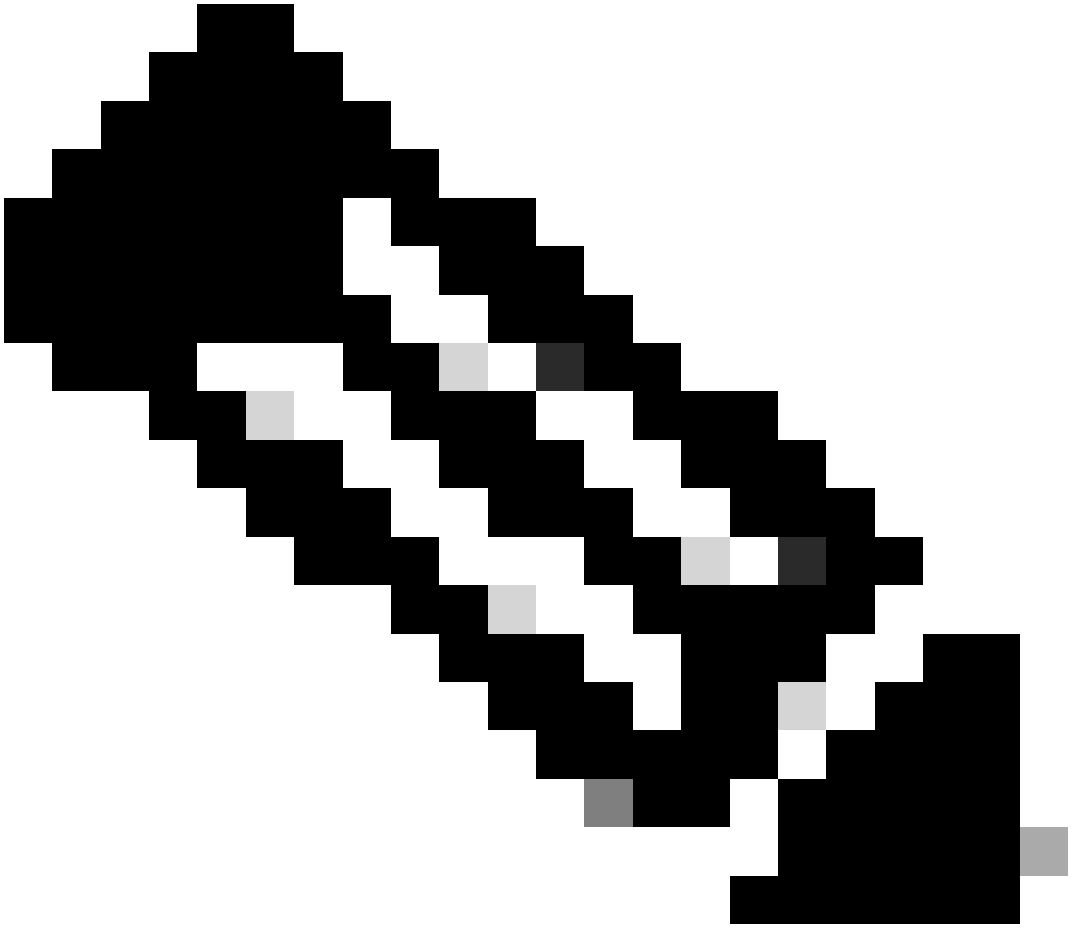
Allow TLS 1.0, 1.1 and 1.2 : active TLS 1.0, 1.1 and 1.2 pour les services suivants. Autoriser également les chiffrements SHA-1 : permet aux chiffrements SHA-1 de communiquer avec des homologues pour ces flux de travail :

- Authentification EAP.
- Téléchargement CRL à partir du serveur HTTPS.
- Communication Syslog sécurisée entre ISE et le serveur Syslog externe.
- ISE comme client LDAP sécurisé.
- ISE comme client ODBC sécurisé.
- Services ERS.
- services pxGrid.
- Tous les portails ISE (par exemple, Guest Portal, Client Provisioning Portal, MyDevices

Portal).
- Communication MDM.
- Communication passiveID Agent.
- Approvisionnement de l'autorité de certification
- Accès à l'interface utilisateur administrateur.

Ces ports sont utilisés par les composants répertoriés en haut pour la communication :

- Accès administrateur : 443
- Ports Cisco ISE : 9002, 8443, 8444, 8445, 8449 ou tout port configuré pour les ports ISE.
- ERS : 9060, 9061, 9063
- pxGrid : 8910



Remarque : l'option Allow SHA-1 Ciphers est désactivée par défaut. Nous vous recommandons d'utiliser des chiffrements SHA-256 ou SHA-384 pour une sécurité renforcée.

Vous devez redémarrer tous les noeuds d'un déploiement après avoir activé ou désactivé l'option Allow SHA-1 Ciphers. Si le redémarrage échoue, les modifications de configuration ne sont pas appliquées.

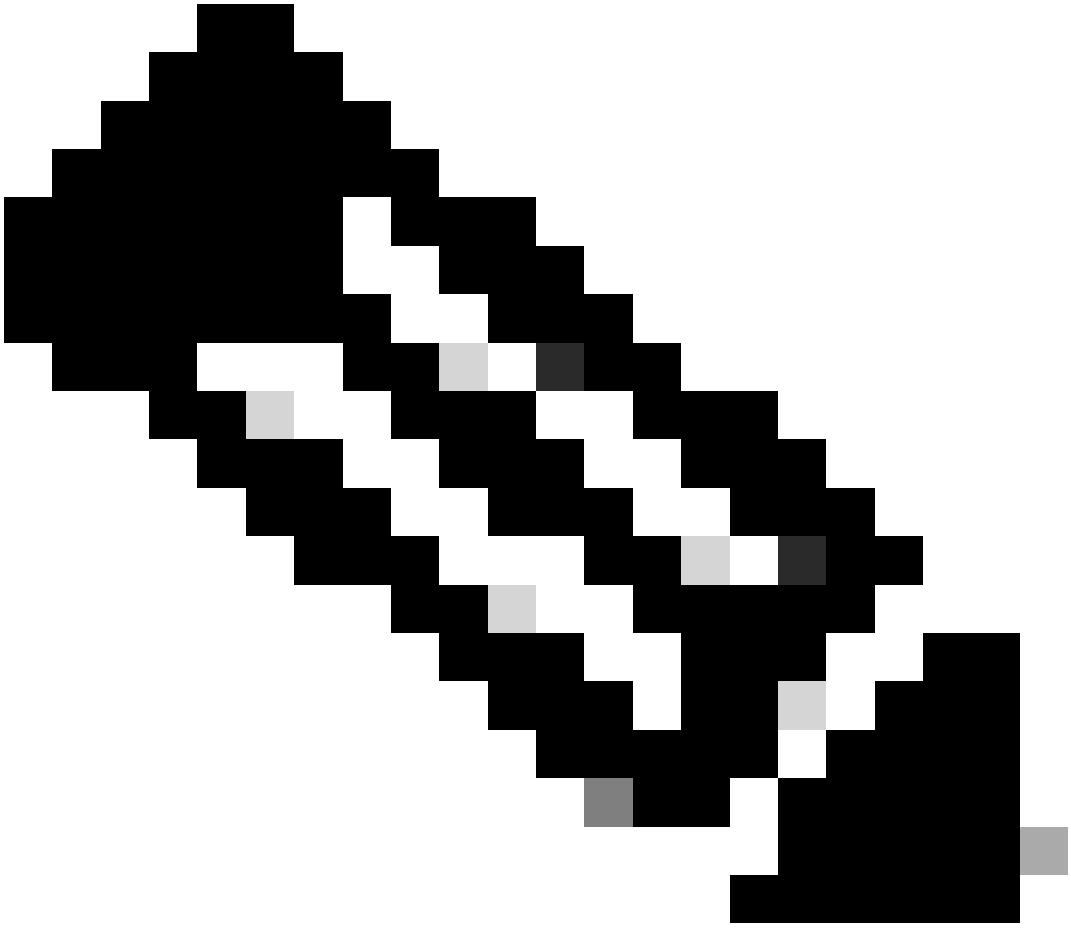
Lorsque l'option Allow SHA-1 Ciphers est désactivée, si un client avec seulement des chiffrements SHA-1 tente de se connecter à Cisco ISE, la connexion échoue et vous pouvez voir un message d'erreur sur le navigateur du client.

Choisissez l'une des options tout en autorisant les chiffrements SHA-1 à communiquer avec les homologues hérités :

- Allow all SHA-1 Ciphers : permet à tous les chiffrements SHA-1 de communiquer avec les homologues hérités.
- Allow only TLS_RSA_WITH_AES_128_CBC_SHA : autorise uniquement le chiffrement TLS_RSA_WITH_AES_128_CBC_SHA à communiquer avec les homologues hérités.

Allow TLS 1.3 : autorise TLS 1.3 pour l'accès HTTPS administrateur sur le port 443 pour :

- Interface utilisateur graphique d'administration Cisco ISE
- API activées pour le port 443 (Open API, ERS, MnT).



Remarque : les communications AAA et tous les types de communications entre noeuds ne prennent pas en charge TLS 1.3. Activez TLS 1.3 sur Cisco ISE et les clients et serveurs appropriés pour l'accès administrateur sur TLS 1.3.

Autoriser les chiffrements ECDHE-RSA et 3DES : permet aux chiffrements ECDHE-RSA de communiquer avec des homologues pour ces workflows :

- Cisco ISE est configuré comme serveur EAP
- Cisco ISE est configuré en tant que serveur RADIUS DTLS
- Cisco ISE est configuré en tant que client RADIUS DTLS
- Cisco ISE télécharge la liste de révocation de certificats depuis HTTPS ou un serveur LDAP sécurisé
- Cisco ISE est configuré comme client syslog sécurisé

- Cisco ISE est configuré comme client LDAP sécurisé

Autoriser les chiffrements DSS pour ISE en tant que client : lorsque Cisco ISE agit en tant que client, permet aux chiffrements DSS de communiquer avec un serveur pour ces flux de travail :

- Cisco ISE est configuré en tant que client RADIUS DTLS
- Cisco ISE télécharge la liste de révocation de certificats depuis HTTPS ou un serveur LDAP sécurisé
- Cisco ISE est configuré comme client syslog sécurisé
- Cisco ISE est configuré comme client LDAP sécurisé

Allow Legacy Unsafe TLS Renegotiation for ISE as a Client : permet la communication avec les serveurs TLS hérités qui ne prennent pas en charge la renégociation TLS sécurisée pour ces flux de travail :

- Cisco ISE télécharge la liste de révocation de certificats depuis HTTPS ou un serveur LDAP sécurisé
- Cisco ISE est configuré comme client syslog sécurisé
- Cisco ISE est configuré comme client LDAP sécurisé

Divulguer les noms d'utilisateur non valides : par défaut, Cisco ISE affiche le message non valide pour les échecs d'authentification en raison de noms d'utilisateur incorrects. Pour faciliter le débogage, cette option force Cisco ISE à afficher les noms d'utilisateur dans les rapports, au lieu du message non valide. Notez que les noms d'utilisateur sont toujours affichés pour les échecs d'authentification qui ne sont pas dus à des noms d'utilisateur incorrects.

Cette fonctionnalité est prise en charge pour les sources d'identité Active Directory, Utilisateurs internes, LDAP et ODBC. Il n'est pas pris en charge pour les autres sources d'identité, telles que le jeton RADIUS, RSA ou SAML.

Utiliser des certificats basés sur FQDN pour communiquer avec des fournisseurs tiers (TC-NAC) : les certificats basés sur FQDN doivent respecter les règles suivantes :

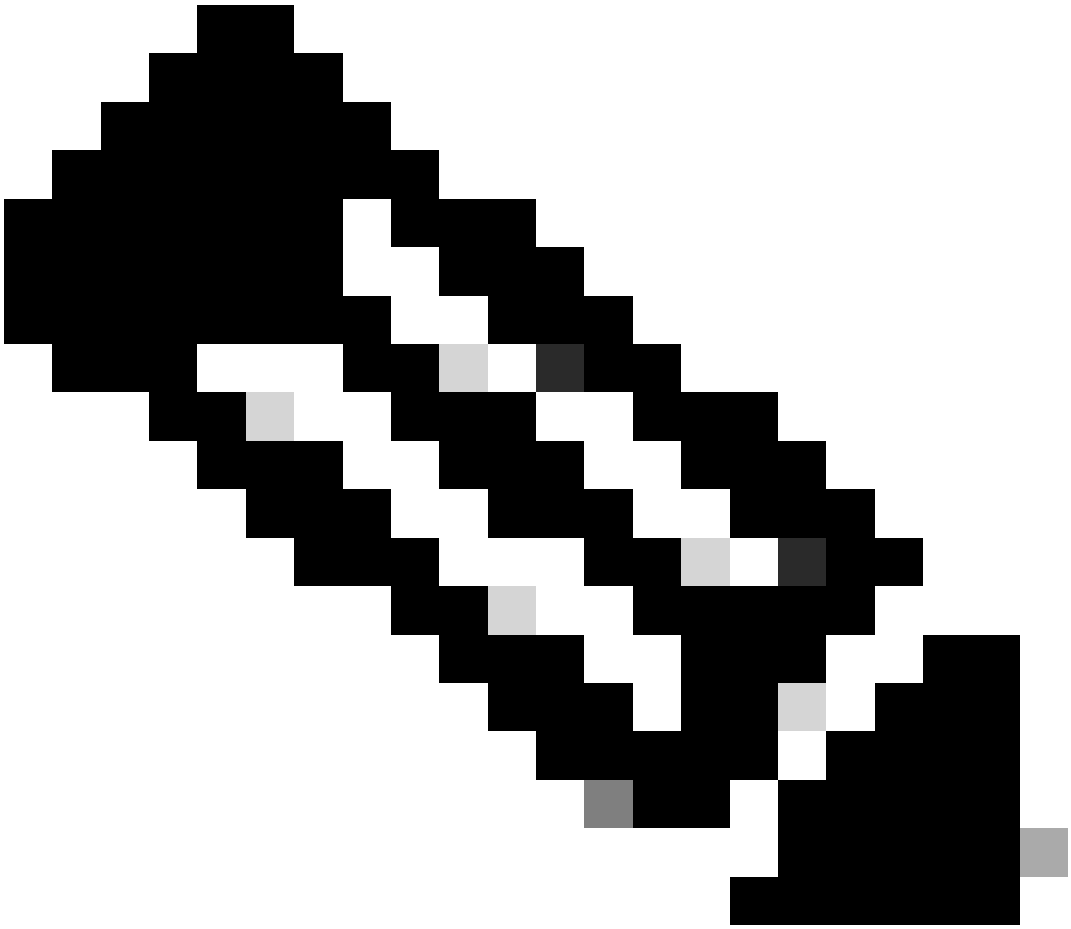
- Les champs SAN et CN du certificat doivent contenir des valeurs FQDN. Les noms d'hôte et les adresses IP ne sont pas pris en charge.
- Les certificats génériques doivent contenir le caractère générique uniquement dans le fragment le plus à gauche.
- Le nom de domaine complet fourni dans un certificat doit pouvoir être résolu par DNS.

Désactiver les chiffrements spécifiques

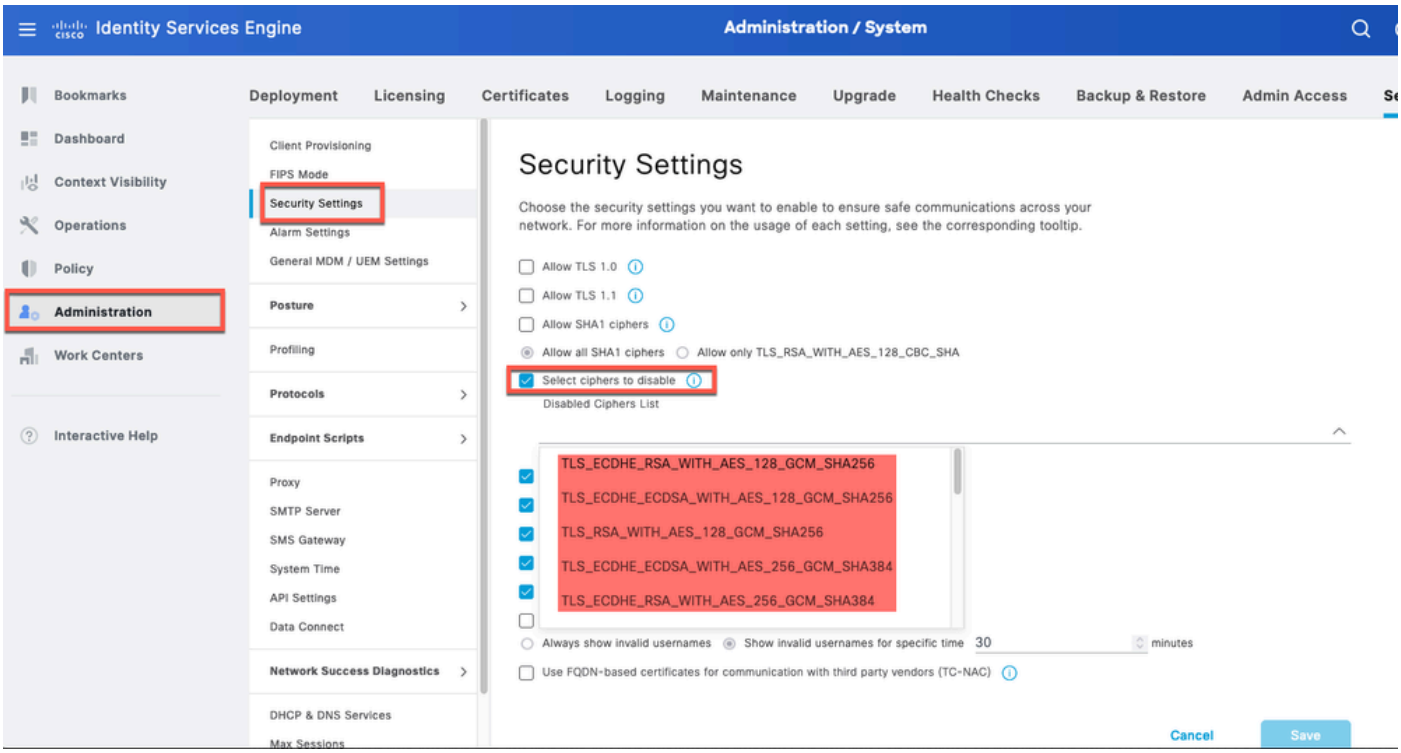
Cochez l'option Manually Configure Ciphers List si vous voulez configurer manuellement les chiffrements pour communiquer avec ces composants Cisco ISE : interface utilisateur d'administration, ERS, OpenAPI, Secure ODBC, portails et pxGrid. Une liste de chiffrements est

affichée avec les chiffrements autorisés déjà sélectionnés. Par exemple, si l'option Allow SHA1 Ciphers est activée, les chiffrements SHA1 sont activés dans cette liste. Si l'option Allow Only TLS_RSA_WITH_AES_128_CBC_SHA est sélectionnée, seul ce chiffre SHA1 est activé dans cette liste. Si l'option Allow SHA1 Ciphers est désactivée, vous ne pouvez pas activer de chiffrement SHA1 dans cette

---



Remarque : lorsque vous modifiez la liste des chiffrements à désactiver, le serveur d'applications redémarre sur tous les noeuds Cisco ISE. Lorsque le mode FIPS est activé ou désactivé, les serveurs d'applications sur tous les noeuds sont redémarrés, ce qui entraîne une interruption importante du système. Si vous avez désactivé des chiffrements à l'aide de l'option Manually Configure Ciphers List, vérifiez la liste des chiffrements désactivés après le redémarrage des serveurs d'applications. La liste des chiffrements désactivés n'est pas modifiée en raison de la transition du mode FIPS.



Option de désactivation du chiffrement ISE 3.3

- À partir de l'interface de ligne de commande ISE, vous pouvez exécuter la commande application configure iseet utiliser l'option 37, mise en surbrillance dans cette capture d'écran, **Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS**. Le bogue associé est l'ID de bogue 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
```

Option de désactivation/activation de RSA_PSS pour EAP-TLS

Informations connexes

-

Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.