

# Mode PAP sur ISE

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez le mode PAP sur ISE](#)

[Problèmes courants tout en activant le mode PAP](#)

[Problème](#)

[Solution](#)

[Problème](#)

[Solution](#)

## Introduction

Ce document décrit les protocoles conformes des Normes fédérales pour le traitement de l'information (PAP) relatif à l'engine de Service d'identité (ISE) et les problèmes courants ont rencontré tout en activant des PAP. Les PAP sont les normes qui sont développées par le gouvernement fédéral des Etats-Unis pour l'usage dans des systèmes informatiques par les organismes publics et les contacteurs non militaires de gouvernement.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### [Composants utilisés](#)

Les informations dans ce document sont basées sur la version ISE 2.1.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Configurez le mode PAP sur ISE

Afin d'assurer le déploiement ISE est des PAP conformes, il y a une option dans ISE d'activer le mode PAP, naviguent vers la **gestion > le système > les configurations > les PAP**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a navigation menu with 'Client Provisioning' selected. The main content area is titled 'FIPS Mode' and shows a dropdown menu for 'FIPS Mode' set to 'Enabled'. There are 'Save' and 'Reset' buttons below the dropdown.

En ce mode, seulement on permet aux les quelques protocoles sélectionnés répertoriés ici pour être utilisé pour des authentications.

- EAP-TLS
- PEAP
- EAP-FAST
- EAP-TTLS

Remarque: Le L-bit Protocol d'EAP-TLS n'est pas des PAP conformes et n'est pas autorisé en mode PAP.

Remarque: On ne permet pas l'option anonyme de ravitaillement PAC dans l'EAP-FAST en mode PAP.

Remarque: Les Certificats et les clés privées doivent utiliser seulement les informations parasites conformes et les algorithmes de chiffrement PAP. Les clés privées devraient être plus grandes que 1024 octets de longueur.

## Problèmes courants tout en activant le mode PAP

### Problème

Protocoles permis utilisant les protocoles non-PAP conformes.

Message d'erreur : « « Les protocoles permis suivants » sont configurés pour utiliser les protocoles non-PAP conformes. Des PAP ne peuvent pas être activées jusqu'à ce que ceux-ci « des protocoles permis » soient supprimés ou elles sont éditées pour utiliser seulement des protocoles conformes PAP. »



The following "Allowed Protocols" are configured to use non-FIPS compliant protocols. FIPS can not be enabled until these "Allowed Protocols" are deleted or they are edited to use only FIPS compliant protocols.

## Solution

Edit a permis à des protocoles pour désactiver des protocoles non-conformes.

Naviguez vers la **stratégie > les éléments > les résultats > l'authentification de stratégie > des protocoles permis**.

Ces services peuvent être supprimés ou édités pour ne pas utiliser des protocoles non-conformes PAP.

Les cases greyed de sortie des protocoles dans cette image ne sont pas des PAP conformes. Seulement ceux qui ne sont pas greyed peuvent être utilisés en mode PAP.

Process Host Lookup ⓘ

### Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

Allow LEAP

Allow PEAP

Allow EAP-FAST

Allow EAP-TTLS

Preferred EAP Protocol

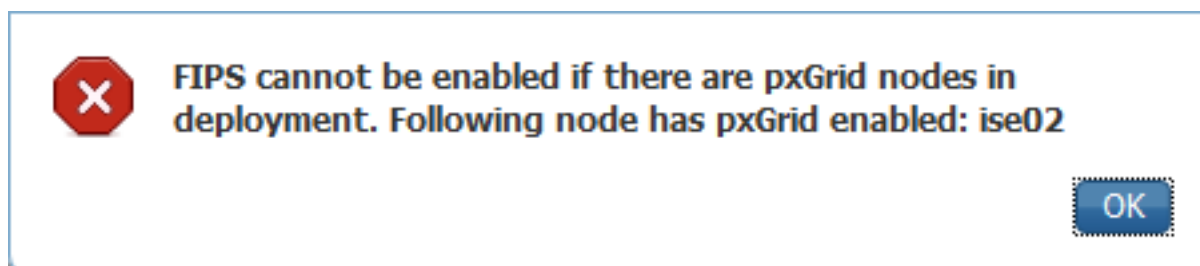
EAP-TLS L-bit ⓘ

Allow weak ciphers for EAP ⓘ

## Problème

Des PAP ne peuvent pas être activées s'il y a des Noeuds de pxGrid dans le déploiement.

Message d'erreur :



## Solution

## Person de PxGrid de débranchement sur tous les Noeuds

Le service de PxGrid n'est pas conforme avec des normes PAP. Par conséquent, le pxGrid ne peut pas être activé sur les Noeuds l'uns des dans le déploiement.

Afin de désactiver le service de pxGrid, naviguez vers la **gestion > le système > le déploiement**. Sélectionnez les Noeuds mentionnés dans l'erreur et décochez la Person de pxGrid pour ce noeud et sauvegardez la configuration suivant les indications de l'image.

Hostname **ise02**  
FQDN **ise02.raghav.com**  
IP Address **10.106.73.104**  
Node Type **Identity Services Engine (ISE)**

---

**Personas**

Administration      Role **STANDALONE**     

Monitoring      Role **PRIMARY**      Other Monitoring Node

Policy Service

Enable Session Services           

Enable Profiling Service

Enable SXP Service      Use Interface **GigabitEthernet 0**     

Enable Device Admin Service     

Enable Identity Mapping     

pxGrid