

# Modo FIP no ISE

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar o modo FIP no ISE](#)

[Problemas comuns ao permitir o modo FIP](#)

[Problema](#)

[Solução](#)

[Problema](#)

[Solução](#)

## Introdução

Este documento descreve os protocolos complacentes dos padrões de processamento de informação federal (FIP) no motor de Service da identidade (ISE) e os problemas comuns encontrados ao permitir FIP. Os FIP são os padrões que são desenvolvidos pelo governo federal do Estados Unidos para o uso nos sistemas de computador por agências do governo e por contadores NON-militares do governo.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

A informação neste documento é baseada na versão do 2.1 ISE.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar o modo FIP no ISE

A fim assegurar o desenvolvimento ISE é FIP complacentes, há uma opção no ISE para girar sobre o modo FIP, navega à **administração > ao sistema > aos ajustes > aos FIP**.

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 options like 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'PassiveID'. 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. The left sidebar also shows 'Client Provisioning', 'Alarm Settings', 'Posture', 'Profiling', and 'Protocols'.

Neste modo, somente poucos protocolos selecionados alistados aqui são permitidos ser usados para autenticações.

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

**Note:** O protocolo do L-bit do EAP-TLS não é FIP complacentes e não é permitido no modo FIP.

**Note:** A opção anônima do abastecimento PAC em EAP-FAST não é permitida no modo FIP.

**Note:** Os Certificados e as chaves privadas devem usar somente a mistura complacente e os algoritmos de criptografia FIP. As chaves privadas devem ser maiores de 1024 bytes de comprimento.

## Problemas comuns ao permitir o modo FIP

### Problema

Protocolos permitidos usando NON-FIP protocolos complacentes.

Mensagem de erro: “Os seguintes “protocolos permitidos” são configurados para usar os protocolos NON-FIP complacentes. Os FIP não podem ser permitidos até que estes “protocolos permitidos” estejam suprimidos ou estiverem editadas para usar somente protocolos complacentes FIP.”



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.

## Solução

Edit permitiu que os protocolos desabilitassem protocolos NON-complacentes.

Navegue à política > aos elementos > aos resultados > à autenticação da política > protocolos permitidos.

Estes serviços podem ser suprimidos ou editado para não usar protocolos NON-complacentes FIP.

As caixas de seleção desabilitada da saída dos protocolos nesta imagem não são FIP complacentes. Somente esses que não são desabilitada para fora podem ser usados no modo FIP.

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

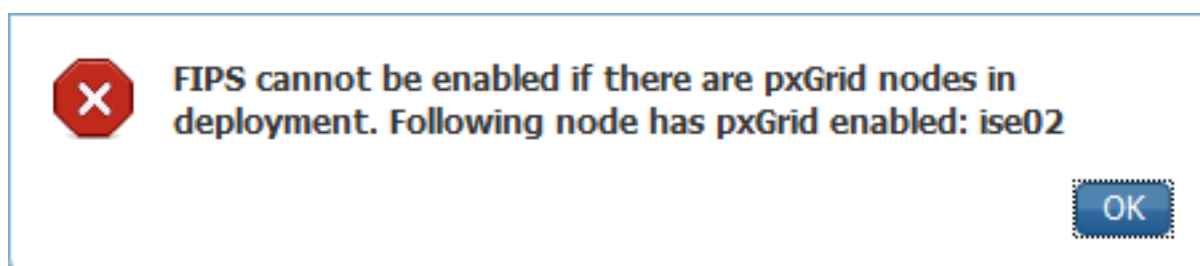
EAP-TLS L-bit ⓘ

Allow weak ciphers for EAP ⓘ

## Problema

Os FIP não podem ser permitidos se há uns Nós do pxGrid no desenvolvimento.

[Mensagem de Erro:](#)



## Solução

## Personalidade de PxGrid do desabilitação em todos os Nós

O serviço de PxGrid não é complacente com padrões FIP. Daqui, o pxGrid não pode ser permitido em alguns dos Nós no desenvolvimento.

A fim desabilitar o serviço do pxGrid, navegue à **administração > ao sistema > ao desenvolvimento**. Selecione os Nós mencionados no erro e desmarcar a personalidade do pxGrid para esse nó e salvar a configuração segundo as indicações da imagem.

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