

Режим FIPS на ISE

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройте режим FIPS на ISE](#)

[Типичные проблемы при включении режима FIPS](#)

[Проблема](#)

[Решение](#)

[Проблема](#)

[Решение](#)

Введение

Этот документ описывает Федеральные стандарты обработки информации (FIPS) (FIPS) совместимые протоколы на Идентичности механизме Service (ISE) и типичных проблемах, с которыми встречаются при включении FIPS. FIPS является стандартами, которые разработаны Федеральным правительством Соединенных Штатов для использования в компьютерных системах агентствами невоенного правительства и правительственными контакторами.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на ISE 2. 1, Version.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройте режим FIPS на ISE

Чтобы гарантировать, что развертываниями ISE является совместимый FIPS, существует опция в ISE, чтобы включить режим FIPS, перейти к **администрированию> Система> Параметры настройки> FIPS**.

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 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'PassiveID'. The 'Settings' option is selected. The main content area is titled 'FIPS Mode' and shows a dropdown menu set to 'Enabled' with a green checkmark icon. Below the dropdown are 'Save' and 'Reset' buttons. The left sidebar contains a navigation menu with 'Client Provisioning', 'Alarm Settings', 'Posture', 'Profiling', and 'Protocols'.

В этом режиме только нескольким выбранным протоколам, перечисленным здесь, позволяют использоваться для аутентификаций.

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

Примечание: EAP-TLS Протокол L-bit не является совместимым FIPS и не позволен в режиме FIPS.

Примечание: Анонимная опция инициализации PAC в EAP-FAST не позволена в режиме FIPS.

Примечание: Сертификаты и секретные ключи должны использовать только FIPS совместимый хэш и алгоритмы шифрования. Секретные ключи должны быть больше, чем 1024 байта в длине.

Типичные проблемы при включении режима FIPS

Проблема

Разрешенные протоколы с помощью не-FIPS совместимые протоколы.

: 'Следующие "Разрешенные протоколы" настроены для использования не-FIPS совместимые протоколы. FIPS не может быть включен, пока эти "Разрешенные протоколы" не удалены, или они отредактированы для использования только FIPS совместимые протоколы!'



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.

Решение

Отредактируйте разрешенные протоколы для отключения не соответствующих стандарту протоколов.

Перейдите к Политике > Элементы Политики > Результаты > Аутентификация > Разрешенные протоколы.

Эти сервисы могут или быть удалены или отредактированы для не использования FIPS не соответствующие стандарту протоколы.

Отображенными серым флажками протоколов в этом образе не является совместимый FIPS. Только те, которые не отображены серым, могут использоваться в режиме FIPS.

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 ⓘ

Проблема

Если существуют pxGrid узлы в развертываниях, FIPS не может быть включен.

:



FIPS cannot be enabled if there are pxGrid nodes in deployment. Following node has pxGrid enabled: ise02

OK

Решение

Отключите персону PxGrid на всех узлах

Сервис PxGrid несовместим со стандартами FIPS. Следовательно, pxGrid не может быть включен ни на одном из узлов в развертываниях.

Для отключения pxGrid Сервиса перейдите к **администрированию**> **Система**> **Развертывания**. Выберите узлы, упомянутые по ошибке, и снимите флажок с pxGrid персоной для того узла и сохраните конфигурацию как показано в образе.

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