IBM WebSphere Commerce V7 FEP7

NIST SP 800-131A Compliance Overview

Contents

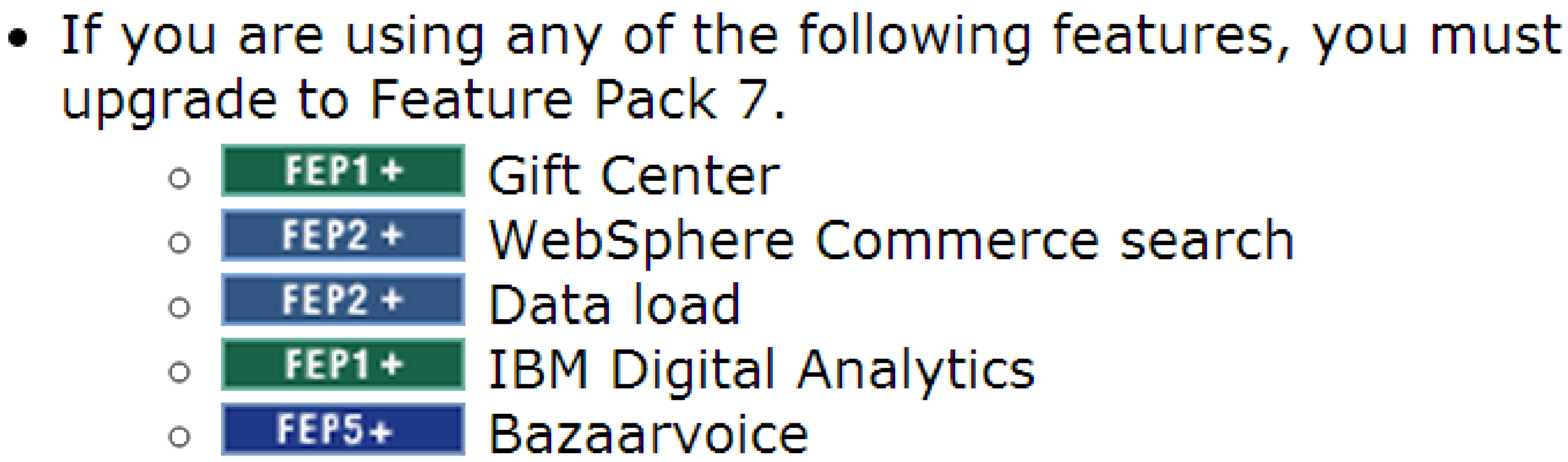
- Overview
- Prerequisites
- Enablement steps
- Reference

Overview

- IBM software products need to comply with the requirements as defined by National Institute of Standards and Technology (NIST) Special Publications 800-131A (required by US Federal customers)
- SP 800-131A strengthens security by defining which algorithms can be used and their minimum strengths.
- The new NIST SP 800-131A standards will be mandatory for US Federal Customers beginning 2014

Prerequisites

- WebSphere Commerce fix pack 7.0.0.8 which now requires WAS 7.0.0.29



- If you are using any of the following features, you must upgrade to Feature Pack 7.
  - FEP1 + Gift Center
  - FEP2 + WebSphere Commerce search
  - FEP2 + Data load
  - FEP1 + IBM Digital Analytics
  - FEP5+ Bazaarvoice

Enablement step 1

1. **Encryption**
   - Encryption must have a minimum key strength of 112 bits
   - Default Encryption algorithm in WC is Triple DES which is still acceptable for PCI Compliance
   - AES is a newer, faster encryption algorithm, which is widely used in the industry
     - AES-128 bit encryption is used if the customer decides to be NIST SP800-131A compliant
   - MigrateEncryptedInfo utility must be run to migrate data in the database to AES
     - This can be done while site is **online**, if key versioning feature is used
   - MigrateEncryptedFiles utility is used to migrate the encrypted data in configuration files, eg. passwords, merchant key, etc.
     - This must be done while site is **offline**

Enablement steps 2 and 3

2. **Message Digest (Hashing) and Digital Signatures**
   - SHA-1 algorithms must be replaced with at least SHA-256, for new data. Existing data can continue to be read using SHA-1
   - Currently SHA-1 is used for hashing passwords, and comparing digital signatures.
   - Switching to SHA-256 involves updating the instance configuration file and wcs_password command line utility

3. **Use of TLS 1.2 for Secure Socket Layer (SSL)**

- Enable TLS 1.2 and be prepared to disable protocols less than TLS 1.2
  - Turn on SP 800-131 in WAS Admin Console in strict mode
  - Ensure **web server** supports TLS 1.2, eg. IHS 8.5.5
    - In the process of making this available to WC 7 customers
  - Ensure the **browser** supports TLS 1.2, eg. IE 8+ on Windows 7
    - Most browsers do not support this by default, so if you only allow TLS 1.2, most shoppers would be blocked from your site

Enablement step 4

4. **Certificates**
   - Ensure that all certificates are created with a key of sufficient strength: Any certificate using RSA or DSA keys shorter than 2048-bits needs to be replaced with a certificate using 2048-bit or higher. Certificates using elliptic curve keys shorter than 160-bits must be replaced with longer keys. See your certificate authority issuer (CA) for new certificates.
   - Ensure that all certificates are signed by an allowed signature algorithm, for example, SHA-256, SHA-384, SHA-512. **Note**: SHA-1 digest algorithms are not allowed.
   - It is anticipated that customers will likely be required to obtain new certificates in order to comply with SP800-131a

Reference

- NIST SP 800-131A Enablement Steps in the Infocenter:
  - http://pic.dhe.ibm.com/infocenter/wchelp/v7r0m0/topic/com.ibm.commerce.admin.doc/tasks/tsenist800enable.htm