FEBRUARY 2013

Good For Enterprise System

Product Description

1. Good for Enterprise (GFE) is a mobile application and associated server side software intended to act as a secure data container on a mobile device. It provides functionality to ensure data is cryptographically protected in transit between the device and corporate network as well as on the device when the application is locked. GFE also provides Mobile Device Management (MDM) functionality to configure and manage a fleet of corporate mobile devices.

2. The evaluated version is:

   a. Mobile Client: 2.1.1

   b. Good Mobile Control: 2.3.0.402

   c. Good Messaging Server: 7.1.0.34 for Exchange, 6.5.3.10 for Domino.

Evaluation Scope

3. The scope of the DSD Cryptographic Evaluation (DCE) was limited to the GFE application installed on a device running Apple iOS 5.1 or higher configured in accordance with the iOS Hardening Configuration Guide available at http://www.dsd.gov.au/publications/iOS5_Hardening_Guide.pdf. Consequently, this consumer guide only applies to devices that meet these requirements.

4. The scope of the DCE included the following functionality:

   a. Authentication to the container

   b. Secure generation and handling of key material

   c. Encryption of data within the secure container

   d. Encryption of data in transit between the mobile device and corporate network

   e. Mobile Device Management

Common Criteria Certification - Summary

5. At the time of this Protect product's publication the GFE product had not completed the Common Criteria (CC) program evaluation. The work undertaken by DSD as a part of this cryptographic

evaluation was expanded beyond the normal scope and as such DSD advises that this product may be used in accordance with this consumer guide.

DSD Findings and Recommendations

6. The secure container component was found to be suitable for reducing the storage and physical transfer requirements of mobile devices containing PROTECTED information to an UNCLASSIFIED level in accordance with the Cryptography section of the Information Security Manual (ISM). Furthermore, the device-to-corporate-network tunnel can be used to communicate PROTECTED information over public network infrastructure.

7. GFE currently includes a cloud based MDM solution. Consequently, the MDM component of GFE cannot be configured in accordance with the iOS Hardening Configuration Guide, and is therefore suitable for managing devices only containing UNCLASSIFIED (DLM) information. For devices containing PROTECTED information, an on-premise MDM must be used. Agencies are encouraged to review DSD's advice which can be found at http://www.dsd.gov.au/infosec/cloudsecurity.htm to better understand the risks associated with using cloud based MDM providers.

8. On PROTECTED devices, administrators must configure the device policy in the Good Mobile Control server as follows:

a. Under the 'General Polices > Handheld Authentication' page
   i. choose the 'Password protected' radio button
   ii. choose 'Require minimum length of (at least) 11 characters'
   iii. check 'Require both letters and numbers'
   iv. check 'Require both upper and lower case'
   v. check 'Require at least one special character'
   vi. choose 'Require password when idle for more than 5 minutes (or less)'
   vii. choose 'After 5 (or less) invalid password attempts: Lock out user (or Wipe handheld data)'
   viii. if the name and phone number association of a contact could be classified, uncheck 'Allow access to Good Contacts (numbers only) for dialling'

b. Under the 'General Policies > Messaging' page
   i. if any contact information could be classified, uncheck 'Enable access to Good contacts'
   ii. if any calendar information could be classified, uncheck 'Allow event reminder details over lock screen'.

iii. check 'Do not allow data to be copied from the Good application'

c. Under the 'General Policies > Provisioning' page

i. uncheck 'Send welcome email when OTA PIN is created'. Alternatively, change the email template to either exclude the OTA PIN or apply an appropriate protective marking to classify the email as per paragraph 11.

d. Under the 'General Policies > File Handling' page

i. choose the 'Disable all importing and exporting' radio button

9. Furthermore, device administrators should:

a. add a compliance rule to quit or wipe the secure container if a jailbreak is detected. This can be configured under 'Application Policies > Compliance Manager > Add Rule'

b. assess the business requirements and security implications of the other settings to determine the appropriate configuration.

10. It is important to note that policies found under the 'Plugin Policies > iOS Configuration' page apply to the MDM functionality of GFE and not the secure container functionality. As stated above, for PROTECTED deployments, this functionality must be implemented by an on-premise MDM.

11. The following variables must be handled and communicated (where applicable) with the same requirements that apply to the highest classification of data to be stored within the container:

a. The user password

b. The OTA PIN

c. The admin response code required to perform the remote unlock function

12. If the ability to send SMS messages is enabled, users must not send classified SMS messages.

13. Recommendations given in this consumer guide take precedence over those in the ISM where there is a conflict.

Contact

For further information regarding the certification, cryptographic evaluation or compliance with the Information Security Manual please contact DSD on 1300 CYBER1 (1300 292 371) or email dsd.assist@defence.gov.au.

ISM

The advice given in this document is in accordance with the ISM. Australian government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/infosec/ism/index.htm

Consumer Guide

This Consumer Guide was issued on 20 February 2013 by DSD