SYSTEM CENTER MOBILE DEVICE MANAGER 2008 - SERVICE PACK 1

Product Description

System Center Mobile Device Manager 2008 – Service Pack 1 (SCMDM) is a product that is designed to provide a secure management and monitoring solution for Windows Mobile-powered devices.

SCMDM is an enterprise server solution which provides secure data and network access for a mobile workforce, while retaining a high degree of control over mobile device usage. It has over 130 policies, settings and built-in mechanisms that help prevent the misuse of corporate data. SCMDM provides a single point for security-enhanced, behind the firewall access to corporate data and 'line of business' applications.

SCMDM expands on the previous version of the product by incorporating security updates and providing the capability for a Windows Mobile user on a managed device to request an authentication reset of their PIN.

Scope of Evaluation

The scope of the Common Criteria (CC) certification included the following security functionality:

- Device security management
- Device configuration management
- Mobile VPN capability
- SCMDM management

The functions and services that have not been evaluated include:

- Server operating systems and hardware;
- Windows Mobile devices and MDM client software;
- Database server;
- Windows Software Update Server (WSUS);
- Certificate services;
- Active Directory domain service;
- Line of Business application servers;
- Web publishing server;
- Management console;
- Internet Information Services; and

- Group Policy Management Console (GPMC) and Group Policy extensions.

The evaluated product is System Center Mobile Device Manager 2008 - Service Pack 1.

Common Criteria Certification Summary

The product has met the requirements of Common Criteria Evaluation Assurance Level (EAL) 4 augmented with systematic flaw remediation (ALC_FLR.3).

DSD's Cryptographic Evaluation

DSD is required to perform a cryptographic evaluation on the product in addition to the Common Criteria certification. The DSD Cryptographic Evaluation is progressing

DSD's Recommendations

As the DSD cryptographic evaluation has yet to be completed, SCMDM 2008 can only be used as follows:

Windows Mobile Devices

In conjunction with appropriately evaluated Windows Mobile devices and in accordance with their DSD Consumer Guides.

Data in Transit

To downgrade the requirements for data in transit from RESTRICTED and IN-CONFIDENCE to UNCLASSIFIED. SCMDM 2008 may only be connected to RESTRICTED, IN-CONFIDENCE or UNCLASSIFIED agency networks.

Data at Rest

The SCMDM is not required to reduce handling requirements for data at rest on servers therefore no guidance is provided or required.

Agencies wishing to use SCMDM 2008 should also refer to ISM policy on:

- Using electronic mail,
- Portable electronic devices and laptops, and
- Remote access.

Agencies should also be aware of AGIMO guidance on protective marking. These are the Implementation Guide for Email Protective Markings for Australian Government Agencies and Email Protective Marking Standard for the Australian Government. These can be found at the following location:

- http://www.finance.gov.au/publications/protective-markings-and-blackberry-devices-guidance/index.html

Point of Contact

For further information regarding the certification, cryptographic evaluation or compliance with ISM security policy, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

Information Security Manual

The advice given in this document is in accordance with ISM release date September 2008. Australian Government agencies are reminded to check the latest release of the ISM at www.dsd.gov.au/library/infosec/ism.html to investigate if any changes have taken place.

Date of this Consumer Guide

This consumer guide was issued by DSD on 23 September 2009 and supersedes any previously issued consumer guide.