ISC11D052

Title:	UEA Mobile Device Policy - amendment
Author:	Raymond Scott
Date:	31 May 2012
Circulation:	*ISSC, 12 June 2012*
Agenda:	ISC11A003 - B4
Version:	v1.0
Status:	Open

Issue

Amendments to the UEA Exchange Mobile Device policy, originally approved by ISSC in February 2011.

Recommendation

The Committee is invited to approve the amendments to the policy.

Resource Implications

N/A

Equality and Diversity

The implementation of the amendments to the policy is not expected to impact on any equality groups.

Timing of decisions

It is intended that the revised policy will come into immediate effect once approved by the Committee.

Further Information

Enquiries about the content of the paper should be addressed to Raymond Scott (r.scott@uea.ac.uk) – ext 3651).

Background

The amendments to the policy are to include a section on the functionality for remotely wiping a device, and to increase the number of failed passcode attempts before a device is reset to the factory default to 30. The latter amendment was proposed by the IT Forum, whose members were concerned that the original allowance of 12 attempts was too low.

Discussion

UEA Exchange Mobile Device Policy - Amendment

Overview

The current UEA exchange mobile device policy was sent to ITF for consultation in January 2011. This was subsequently approved by ISSC in February 2011. The policy sets out the need to protect UEA email data (emails, calendar and contacts) on mobile devices that are synchronised with the University Exchange server. Mobile devices are at greater risk of being lost, stolen, left unattended and malware. In most cases mobiles devices by default do not have security policies applied to help prevent unauthorised access such as:

- locking the device after a time period
- prompting for a pincode to gain access to the device
- encrypting the storage area on the device

The policy agreed by ISSC enforces the use of a 6 digit PIN code or lock code on any mobile device that is currently set-up with access to UEA email systems. If the pincode is entered incorrectly 12 times the device is reset to factory settings (but following representations by the IT Forum it is proposed to increase this to 30 attempts). The aim of this is to stop any unauthorised viewing or use of UEA email in scenarios such as when a mobile device is left unattended or if lost.

Changes made to the policy and why?

The policy has been amended to include a section on the functionality for remotely wiping a device. The remote wipe facility is part of the standard installation for Outlook Web Access (OWA). This allows the user to select the mobile device that they have setup to use Active Sync (connecting to UEA Exchange email) and instruct it to reset itself to factory settings. In doing this the device will wipe any data such as emails, photos, music, contacts and settings from its local storage area.

This facility can be used by the user in cases where their mobile device has been lost or stolen. This will allow the user to ensure all of their personal information and UEA emails are removed before malicious attempts are made to access this information.

UEA Exchange server administrators do have the ability to initiate a remote wipe of a device on behalf of a user. This will only occur when requested by the user and explicit permission is given. Individuals will need to confirm their identity before any action is taken.

The remote wipe functionality in OWA has been part of the standard installation and available since MS Exchange 2003 SP2 (introduced in Oct 2005). This functionality has been available to UEA OWA users since this service pack was applied.

The IT Forum on 21st May 2012 expressed concern about the number of password attempts allowed before a device is wiped and agreed to increase this from 12 to 30 (the maximum allowed by Microsoft).

Current Rollout Progress of the Policy

Mobile security policies have now been implemented successfully on all UEA exchange accounts (approx 6000). Throughout the rollout users were informed of the reasons why this policy was being implemented, how it would affect them if they were using active sync and what actions they should perform.

To date IT Helpdesk have received complaints from 1% of users affected stating their personal device should not be affected by security policies implemented if they want to access UEA email. The most contentious issues for these users are the automatic locking of the device after a set period of time along with the need to enter a pincode to unlock the device. 2% of user queried the reasoning for the policy.

Useful Links

- http://www.uea.ac.uk/is/it/mobile-device-security

UEA Exchange Mobile Devices Security Policy

Author: Raymond Scott (ISD)
Date: 14 June 2011
Version: 1.2

This document defines the University's policy on mobile devices configured to synchronise with the UEA Exchange service.

Version history

Version	Date	Note
0.1	25/1/2011	Discussed at ITF
0.2	4/2/2011	Discussed and approved at ISSC
0.3	16/5/2011	Discussed at ITF where given that time locking following passcode failure was not an option, the number of failed attempts increased to 12
0.4	14/6/2011	Revised policy discussed and approved at ISSC
1.0	10/2/2012	Approved policy
1.1	29/2/2012	Revised Policy after consideration during implementation phase (seeking approval for change from ISSC June 2012)
1.2	31/5/2012	Discussed at ITF who requested the number of failed attempts be increased to 30

Introduction

Currently all mobile devices that synchronise with the UEA Exchange service, in order to access e-mail, calendaring and contacts, are configured to remember user credentials and do not prompt for them to be re-entered. The service is designed in this way in order to support the automatic delivery of new items to devices, when they arrive, without having to re-enter credentials every time the device polls the server. As such if mobile devices are not configured with any type of security code, typically a 4 digit pin code, or have a weak strength code such as 0000 or 1234, the device and its contents present a security and confidentiality issue. This is particularly evident if a device is lost, left unattended or stolen. It would allow anyone who obtains such a device unauthorised access to the UEA Exchange email service and potentially secure and confidential information, in addition to being able to send and delete emails on that device. This is not in keeping with generally accepted corporate IT best practice in this area or with the University's Security Policies.

Following the UEA General Information Security Policy (GISP) ITCS are responsible for all centrally managed systems and services. As such we must determine risks, their impact and the managed response required to remove the risk or reduce its impact (GISP1). As such we must ensure that only authorised users can access University computer systems and IT services by providing and implementing authentication mechanisms to control access (GISP4). In turn the University email service must provide the facility for secure and confidential email correspondence (GISP6).

Policy statements

To eliminate this as a security risk, ITCS is recommending implementing an Exchange Security Policy that would be enforced on all mobile devices that synchronise with the UEA Exchange service. The policy applied to the device would enforce the following settings:

- Mobile device requires pass-code
- Minimum pass-code length = 6
- Number of failed pass-code attempts until device is reset to factory default (formatted) = 30
- Time without user input after which pass-code must be re-entered (in minutes) = 5
- Enforce pass-code history (remembers last 3 pass-codes)
- Require encryption on the storage card

- Enable pass-code recovery (user can obtain recovery pass-code via OWA). ** Apple devices do not currently support this feature**
- Enable a remote wipe facility for devices that synchronise to UEA email using Active-Sync. This can be used in the event that a device is lost or stolen and can be activated by the owner of the device through OWA. **In extreme circumstances this can be performed by ISD but only with the explicit consent of the device owner**

Implementation

As Exchange Security Policies can be assigned on a per user or per server basis, a test policy was created and pushed out to a selected group of test user's mobile devices to assess the impact it would have from a compatibility and usability point of view. This was then be tweaked until the settings were deemed compatible from both a user and security perspective. This limited pilot, run throughout October, provided a cross-section of devices and users who provided very valuable feedback. This feedback led to the policy settings currently proposed and provided knowledge of some of the compatibility issues associated with implementation.

Following on from the success of the limited pilot, a wider pilot of ITCS staff and IT Support was implemented on Wednesday 24th November. This wider pilot has highlighted that a significant number of users use their personal mobile devices to access UEA Exchange email services. This has led to some resistance amongst this group of users who feel that such measures should not be applied to these devices. Whilst we acknowledge these concerns, we are obliged to ensure that the security and confidentiality of email and other UEA data stored on mobile devices remains so and is guaranteed. Officially supported mobile devices remain those provided by the University and as such we must ensure that these are secure. Users of personal devices are not being discouraged from continuing to use the service but should stop synchronising with the Exchange email service if they do not wish these settings to be applied.

We now plan to roll this out to all UEA users in a phased manner, ensuring that sufficient time is allocated to ensure the changes are effectively communicated, and users of personal devices have been given the opportunity to remove UEA email settings.